Home Office Report

Technology-Facilitated Intimate Partner Violence: A multidisciplinary examination of prevalence, methods used by perpetrators and the impact of COVID-19.

25 May 2021

Dr Afroditi Pina & Dr Jennifer Storey

Dr Marian Duggan

Dr Virginia Franqueira

University of Kent | Institute of Cyber Security for Society (iCSS)

Home Office

Acknowledgements

The researchers would like to thank the Home Office for supporting and entrusting us to conduct this research. We hope that the outcomes of this research will shed light on Technology Facilitated Intimate Partner Violence, its perpetrators and impact, and that the results will be the impetus for fruitful conversations and positive change.

The researchers would like to acknowledge and thank The Cyber Helpline Responders for taking the time to talk to us and share their experiences and recommendations. We would also like to thank The Cyber Helpline's CEO, Rory Innes, and Director Charlotte Hooper, for their expert advice and support, preparation of data and training offered to our research assistants.

We would also like to thank our research assistants Abby Hare, Gaye Ildeniz, Rachel Tisi, Sadie Todhunter and Cassidy Weekes for their tireless work and invaluable help throughout this project.

List of Tables and Figures

Contents

Executive Summary

A multidisciplinary team of academics from the University of Kent's Institute for Cyber Security in Society (iCSS) received funding from the Home Office Domestic Abuse Perpetrators Fund to conduct research into the perpetration of Technology Facilitated Intimate Partner Violence (TFIPV). The project comprised of 4 workstreams: 1) A Rapid Evidence Assessment (REA) of the evidence base around TFIVP, 2) A thorough analysis of a representative sample of cases of TFIPV as reported to The Cyber Helpline, 3) interviews and surveys with Helpline Responders around their experiences responding to TFIPV and 4) a synthesis of the findings and a visual presentation. Below is a summary of the main project findings according to the first 3 workstreams:

Workstream 1: Findings from the REA

- No unified definition of TFIPV nor a single accepted measurement exists. We identified over 40 different terms describing various forms of TFIPV in the literature reviewed and multiple measurements.
- Lack of definitional synergy causes difficulties in interpreting research results and estimating prevalence rates of TFIPV.
- Research has been predominantly conducted in North America, with some pertaining to Australia, Canada, Spain, Singapore, Peru and the UK. Non-western and diaspora populations are less represented.
- Most studies have been undertaken with adolescents and young adults. Participants over 30 years old are not adequately represented in research. Also, most participants were female.
- Prevalence rates for TFIPV vary considerably (1%-78%) depending on definition, behaviour measured and methodology.
- Being controlled or monitored was the most cited type of victimisation.
- Most victims of TFIPV have experienced at least one behaviour with approximately 30% experiencing multiple types of TFIPV.
- In adolescent age groups, coerced sexting was identified as one of the main victimisation experienced.
- The most frequent technology platforms used by perpetrators of TFIPV are smartphones, Social Networking Sites (e.g., Facebook), email and Global Positioning Systems (GPS).
- Smart home devices (e.g. IoT; home cameras, smart security, Nest thermostats, Alexa, Google Home etc) are being repurposed for TFIPV, and pose a new challenge for policy makers.
- TFIPV perpetration is correlated with offline domestic abuse and IPV perpetration.
- Most common predictors of TFIPV were jealousy, anger/hostility, alcohol consumption/substance abuse and social media use.
- Social media platforms are highlighted as conducive environments for monitoring, controlling and inflammatory behaviours online. Online communications disinhibit some individuals because they are perceived as sanction-free.
- Mutual TFIPV patterns exist in romantic relationships where perpetration and victimisation are experienced in tandem.

- Gender is not a significant predictor for either victimisation or perpetration. There are, however, some differences in motivation and type of TFIPV behaviour perpetrated by men and women. Women tend to perpetrate more covert and less serious forms of TFIPV (such as monitoring a partner's social media or phone) compared to males' more overt and severe TFIPV (e.g., antisocial, predatory, IBSA behaviours).
- Experiencing IPV is the highest vulnerability and risk factor for TFIPV in victims: denotes the need to see TFIPV as part of the umbrella of IPV
- Women report greater impact of TFIPV than men.
- Significant impacts of TFIPV include severe psychological distress, isolation, and a feeling of not being able to escape because of the online format.
- Disabled, culturally and linguistically diverse, learning-disabled and sexual minority victims are at greater risk of TFIPV and may have greater difficulty accessing support.
- Sharing children with perpetrators impacts the level of harassment and intimidation via TFIPV as well as the likelihood to disengage from digital communication settings.
- Professionals responding to TFIPV usually lack the sophisticated technical expertise to help and advise victims on security.
- Lack of standardised protocols for responding to TFIPV, failure to recognise technology use as abusive and advising victims to go offline following TFIPV is linked to re-victimisation and victim blame.

Workstream 2: Findings from The Cyber Helpline Case Analysis

- A total of 666 cases, 89 (13.4%) of which were TFIPV, took place in the year before COVID-19 restrictions were imposed compared to 3,815 cases, 463 (12%) of which were TFIPV, that occurred during COVID-19 restrictions.
- This equates to a 472.8% increase in cases reported to The Cyber Helpline post-COVID-19, and a 420.2% increase in TFIPV cases reported.
- There were 22 types of TFIPV:
    - Classified into 5 attack categories: *Unwanted contact and communication*, *Extortion*, *Unauthorised access*, *Physical device problems* and *Theft*.
    - *Unwanted contact and communication* and *Extortion* were the most common.
    - Categories that differed by relationship type:
        - *Extortion* was more common in brief relationships.
        - *Unwanted contact and communication* and *Unauthorised access* were more common in long term partnerships.
    - Category that differed based on COVID-19 restrictions:
        - Extortion was more common post-COVID-19.
    - Individual TFIPV types that differed by COVID-19 restrictions:
        - *Cyberstalking*, *Unauthorised access to social media* and *the Generic use of malware* were more common pre-COVID-19.

        - *Webcam Blackmail Sextortion* was more common post-COVID-19.

- 21 methods were used by perpetrators to engage in TFIPV and The Cyber Helpline also engaged in preventative assistance to avoid TFIPV.
- Average of 2 methods used per case, with a range of 1-10 methods.
    - Methods could be broadly grouped into 5 groups: *Preventative*, *Communication with the victim*, *Communication about the victim, Technical surveillance* and *Card fraud.*
    - Communicating with the victim was most common.
    - Social media was used as a method of engaging in TFIPV in 171 (30.8%) cases.
        - Of those cases, Facebook (including messenger) was the most common platform used (n = 77, 46.7%).
    - Groups that differed by relationship type:
        - Communication with and about the victim were more common in brief relationships.
    - Groups that differed based on COVID-19 restrictions:
        - Communication with and about the victim were more common post-COVID-19.
    - Individual TFIPV methods that differed by COVID-19 restrictions:
        - *Email contact, Remote access, Monitoring internet use, Spyware, Malware* and *Cameras, bugs and trackers* were significantly more common pre-COVID-19.
        - *Social media, Phone, Fake profile* and *Video call recording* were significantly more common post-COVID-19.

Workstream 3: Synthesised Data Collection from The Cyber Helpline Responders

Patterns Observed in Perpetrators' Modus-Operandi

- Physical access offers new opportunities for TFIPV in a way that is different from other types of harassment (e.g., to install listening devices, to set up and manipulate victims' devices).
- Perpetrators use simple methods and technologies to abuse, often using their knowledge of the victim's online habits and activities (e.g., email, social media, GPS-enabled trackers, family sharing accounts, known passwords).
- Perpetrators are leveraging the increasing presence of home smart devices to track, intimidate, and monitor victims.
- Perpetrators take advantage of trust built naturally over the relationship and use that knowledge against the victim to commit TFIPV when the relationship is over.

- Technology is often used for manipulation of victims in a manner which poses significant psychological impacts (e.g., gaslighting).
- Lack of ID verification by online platforms and the anonymity this offers perpetrators is contributing to the insidiousness of TFIPV
- Perpetrators sometimes commit TFIPV using microphone and recording devices ("bugs") that are cheaply and easily purchased online (e.g., for monitoring purposes).

Impact of COVID-19

- There was an increase in the volume and intensity of TFIPV cases during the lockdown period.
- Victims were less able to avoid being online to escape TFIPV during COVID-19.
- Perpetrators had more time and opportunity to learn and improve their skills for online abuse or to consider different forms of abuse (e.g., for monitoring, tracking) during lockdown.
- Perpetrators adapted their methods to incorporate the practice of sending gifts or unwanted goods to victims as part of their TFIPV activities.

Problematic Factors / Phenomena

- Victims are unduly tasked with collecting and holding evidence of TFIPV, which may have negative impacts on their mental health. Victims also reported feeling embarrassed and responsible (e.g., demonstrating self-blame) which made them reticent to seek help.
- Victims who have reported TFIPV to the police are sometimes frustrated by the response they receive (e.g., lack of follow-up, being told that there is insufficient evidence, being advised to go offline).
- Few resources relating to safeguarding and healthy relationships are available.
- Perpetrators are rarely held to account for their TFIPV behaviours as the current legislation is inadequate.
- Victims face obstacles when trying to establish contact with social media or email providers to counter abuse.

Recommended Interventions

- A multi-agency reporting mechanism would better support victims by allowing a single view of cases while improving perpetrator accountability.
- TFIPV could be reduced with the greater use of secure settings (e.g., multi-factor authentication), or by having these enabled by default on devices and accounts.
- Legislation requires updating to better reflect the nature of TFIPV.
- Police forces require updated, specialist training (e.g., on digital evidence gathering) and greater resourcing to better support TFIPV victims and investigate cases. Some

form of baseline or standardised approach to TFIPV would help improve the regional variation in statutory responses to TFIPV.

- Better Government-imposed regulations and sanctions are required to ensure online service providers take more responsibility in combatting TFIPV. These providers should also improve accessibility to personnel via customer service helpdesks and apply ID verification for users.
- Perpetrators should be provided with help and support to desist engaging in TFIPV.

Introduction

Technology facilitated intimate partner violence (TFIPV) has evolved considerably with developments in both the nature and accessibility of interactive communications. Following the COVID-19 global pandemic and subsequent lockdowns and restrictions, the move to remote working and engagement in online leisure activities provided ample opportunities for perpetrators to harass, monitor, and control their victims online (Yardley, 2020). Research has recognised the use of smartphones, social media and GPS location tracking as examples of technologies used to perpetrate abuse both pre COVID-19 and during it (Douglas, Harris & Dragiewicz, 2019; Gilchrist et al, 2017; Yardley, 2020). While technology may be considered an integral part of intimate partner violence, few studies have been able to chart the increased prevalence rates arising during COVID-19.

The types of TFIPV perpetrated against victims reflects existing offline behaviours, including economic abuse, sexual abuse, emotional abuse and physical violence, with monitoring and control featuring heavily (Freed et al, 2018; Woodlock, 2017). This control usually manifests in the form of monitoring social media; emails; threats to harm the victim, their family or friends; using GPS tools as well as spyware; threatening to or sending intimate imagery/media of the victim; or restricting the victim's internet access and communication with others via technology (Attrill-Smith & Wesson, 2020). Recent Crown Prosecution Service data (CPS, 2020) revealed that stalking is now recognised as a form of DA since the majority of stalking (84%) is committed by ex-partners. Social media was cited as being used in 34% of cases, where multiple online accounts were created by ex-partners to contact the victims and 6% involved "revenge porn" where private images of the victims were shared without their consent. According to the Suzy Lamplugh Trust, all recent reports of stalking made to the charity involved some form of digital stalking, and this form of IPV intensified during the COVID-19 related lockdown (Suzy Lamplugh Blog, 2020).

The project began by assessing the existing research on TFIPV (e.g., controlling technology use, hacking, tracking, image-based abuse, harassment, isolation etc) before exploring what patterns, trends and adaptations perpetrators employed in the period leading up to, and during, the COVID-19 pandemic. The findings inform a range of policy recommendations on TFIPV.

Research Aims

The project 1) identified the evolving methods of abuse involved in TFIPV; 2) determined what types of technology are used, and how, in TFIPV and, 3) explored the types of digital vulnerabilities pertaining to victims which perpetrators exploit. Using these aims, we developed typologies categorising methods of TFIPV perpetration. While existing research has rightly focused on TFIPV victims to identify risk factors, prevalence, and impact, we

identified an urgent need for research on TFIPV perpetrators and their methods. Conducting such research is rendered difficult, as access to online offender populations remains scarce. Furthermore, the reliance on self-reported measures of criminal activity is fraught with socially desirable and biased responding.

Expertise

The project involved a multidisciplinary team of experts in IPV: two psychologist co-leads (Dr Afroditi Pina & Dr Jennifer Storey) with established track records of publications in IPV and online abuse as well as in advising police, government and other stakeholders; one criminologist with an established publication record on IPV who is also a domestic abuse charity trustee (Dr Marian Duggan); and one computer scientist with extensive expertise on cybersecurity and cyberstalking (Dr Virginia Franqueira). These academics partnered with The Cyber Helpline, a not-for-profit organisation staffed by information security professionals who offer free and confidential advice and assistance to UK victims of cybercrime. The Cyber Helpline is the only such service of its kind in the UK.

The academic team are all members of the Kent Institute of Cyber Security for Society (iCSS), a recognised academic centre of excellence in cyber security research (ACE-CSR) by the government's National Cyber Security Centre (NCSC), with experience in collaborations with governmental and industry organisations as well as international researchers and practitioners to produce and promote good practice in cyber-security.

Workstreams

The project's main aim was to identify how perpetrators use technology to commit IPV. To achieve this, the project was divided into three data collection workstreams: A Rapid Evidence Assessment to establish the evidence base for TFIPV (Workstream 1), a thorough analysis of TFIPV cases as reported to The Cyber Helpline (Workstream 2), interviews and a survey detailing The Cyber Helpline Responders' experiences and challenges responding to TFIPV (Workstream 3) and a consolidation of recommendations and a visual representation (infographic) of evidence gathered by this project (Workstream 4).

Workstream 1: Rapid Evidence Assessment (REA) of the available evidence base on Technology Facilitated Intimate Partner Violence (TFIPV)

Introduction and Rationale

Technology usage has unquestionably permeated people's daily routines and has become an integral part in their personal, working and social lives. Global statistics show that as of January 2021 over 4.6 billion people (nearly 60% of the global population) were active Internet users and over 4.2 billion people were active social media users (Statista, 2021a). Smartphones and mobile devices are becoming more accessible, and they are used by over 90% of internet users globally (Statista, 2021b).

While the internet and telecommunications technologies are keeping people connected—during the COVID-19 pandemic, when travel was significantly restricted, a significant proportion of people were able work remotely and communicate daily with loved ones—they have also been increasingly linked with criminal, antisocial and aggressive behaviours and negative mental and physical impacts (Cybersmile Foundation, 2017; Davidson et al., 2019). Researchers and policy makers have started to recognise and focus on the impact that online technologies and the Internet have on the perpetration of criminal activity; how online technologies facilitate perpetration of offline criminal activity as well as how they give rise to new forms of crime (Brown; 2017; Davidson et al., 2019).

Domestic violence and abuse (DVA), also known as intimate partner violence (IPV), is a prevalent form of violence that affects an estimated 1 in 3 women (30%) and around 1 in 10 men (3-20%) worldwide and has been declared a major public health problem and violation of human rights by the World Health Organization (WHO, 2021). While men can be victims of DVA/IPV, statistically, women are more likely to suffer violence at the hands of a male partner (Crown Prosecution Service, 2019); as many as 38% of all female homicides are committed by current or former intimate partners (WHO, 2021). DVA/IPV has devastating consequences for victims, affecting their physical, mental, sexual, and reproductive health.

During the COVID-19 global pandemic, public safety measures included government directives to the public to "stay at home" during a series of national lockdowns. Globally, DVA/IPV advocates, researchers, and organisations, warned that these extraordinary circumstances would force some people to shelter with abusers for prolonged periods of time, consequently leading to an increased risk of abuse (Campbell, 2020; National Domestic Abuse Helpline, 2020; van Gelder et al., 2020). Many countries reported a surge in DVA/IPV related calls to the police, emergency services, shelters and helplines during the lockdown period (US: Tolan, 2020; UK: Refuge, 2020; Australia: Women's Safety New South Wales, 2020; Canada: Global News Canada, 2020). Some reported a 50-70% increase in contact with services, helplines, and websites, and a 50% increase in the risk of violence (Women's Safety New South Wales, 2020). Refuge, the UK's leading specialist domestic abuse service provider,

reported an 950% increase to website visits compared to pre-COVID-19 statistics (Refuge, 2020).

In recent years, research has identified that IPV can be perpetrated not only in proximity by people who share spaces and lives together, but also remotely, by current and former intimate partners who do not live with the victim (Christie & Wright, 2020). A report published by Refuge indicated that in 2019, 72% of women who contacted them or used their services had been subjected to abuse that used or was facilitated by technology. The Kaspersky Security Network (2020) indicated that attempted and completed installations of commercial spyware apps (often referred to as "stalkerware") used in domestic surveillance increased by 373% in 2019 (compared to 2018). These applications can operate covertly on a victim's device and enable perpetrators to access information on the device, including messages, social media, geolocation and real time audio and video recordings. One of the most important points raised by researchers in recent years, and one that significantly impacts the response to the issue, is that the same technology that provides individuals with access to information and support related to IPV, also enables perpetrators to monitor, harass and control their partners (Grimani, Gavine & Moncur, 2020).

The Domestic Abuse Act (2021) has recently been given royal assent. It includes special provisions for the protection of victims and witnesses in legal (criminal and civil) proceedings (e.g., assistance in the case of intimidated and vulnerable witnesses and victims). Importantly, controlling or coercive behaviour and revenge porn offences have been extended to include behaviours from perpetrators who are ex-intimates and threats to distribute private sexual material (Home Office, 2021).

There is a common recognition that, despite efforts to include online crime in legislation, the majority of existing laws predate the Internet (Law Commission, 2018). Therefore, the laws do not accurately reflect victims' experiences and the behaviours involved in perpetration. This highlights the need to recognise and include behaviours that are perpetrated using technological means or via the internet in legislation (Strickland & Dent, 2017). The Online Harms White Paper (Department of Digital, Culture, Media & Sport & Home Office, 2019) brought together advice and ideas from legal scholars, policy makers, Internet providers and technology companies on safety against online harassment, abuse, exploitation, radicalisation and terrorism. The White Paper is intended to detail a comprehensive regulatory framework for online safety, where tech companies will have clear guidance and responsibilities with a statutory duty of care, where the regulator will have power to take enforcement action (Department of Digital, Culture, Media & Sport & Home Office, 2020).

This Rapid Evidence Assessment (REA) was commissioned by the Home Office to complement existing endeavours and better understand the evidence base surrounding the nature and impact of technology on DA/IPV. This body of work identifies and synthesises existing peer-reviewed literature and policy documents that examine abuse between current and ex-intimate partners, facilitated or perpetrated using technological means, referred to from here forward as technology facilitated intimate partner violence (TFIPV), as well as offers recommendations for statutory and voluntary sectors.

Rapid Evidence Assessments

There are many different types of evidence available, with the most popular method of reviewing this being the literature review. However, conventional literature reviews are prone to bias given the obscure nature of inclusion criteria and the potential for researchers to select sources based on personal preference. Alternatively, a REA is considered a more trusted methodology because it employs a specific and comprehensive approach to study selection based on explicit criteria within a short timeframe. One or more independent reviewers employ these criteria to determine the weight of the evidence collected before extracting the data as relevant to the questions guiding the study. The methodology used in a REA is more transparent, verifiable, and reproducible while being less subject to bias, so is considered more robust than the traditional literature review.

Using the REA to Explore TFIPV

The questions informing this REA were determined by PI (Principal Investigator) Dr Afroditi Pina, who led this workstream, guided by the deliverables agreed and in consultation with the research team. These are are as follows:

1. What evidence exists about the nature of the different types of TFIPV experienced by adults?
2. Who are the perpetrators of TFIPV?
3. What are the needs and vulnerabilities of TFIPV victims?
4. What evidence exists about the scope/prevalence of different types of TFIPV experienced by adults?
5. What evidence exists about the impact of these different types of TFIPV experienced by adults?
6. What are the gaps in the research related to TFIPV and what are recommendations for future research, policy, and practice?

The following inclusion criteria were applied:

- Policy papers, research papers, reviews, meta-analyses, monographs, conference proceedings, small group meeting notes that mention/define TFIPV.
- Any publications between 2010 and 2021.
- Any above document that evaluates the nature, scope, prevalence, perpetrators, victims, and impact of TFIPV.
- Any above document that evaluates an intervention for TFIPV.
- Any above document that evaluates the outcomes of TFIPV.

The following exclusion criteria were applied:

- Any studies published before 2010.
- Newspaper articles, non-academic opinion pieces, or articles whose author cannot be determined.
- Any studies that do not include technology as a means for perpetrating IPV.
- Any studies that are not strictly IPV related.
- Any publications not in English.

Search Strategy

Searches were conducted from 09/03/2021 to 24/03/2021, using combinations of different relevant terms to capture literature that could involve TFIPV but not specify it by this name. These terms included: Technology Facilitated Domestic Abuse; Computer Facilitated Domestic Abuse, Cyber, Abuse, Domestic, Online, Intimate Partner Violence, Techno*, Intimate, Victim, Dating, Violence, Digital, Intimate Partner, Relationship, Partner, Control, Coercive, Power, Internet. Databases utilised for this search are shown in Table 1. A basic filter was applied across all databases to return only scholarly and peer-reviewed journals. In addition, a call for materials and studies was made to all known academic and policy links within the group. All search terminologies used across databases with relevant returns are shown in Table 2.

Table 1. Databases used in the Rapid Evidence Assessment search

Databases used in initial search	Further databases checked after initial saturation reached	Policy material sources
Web of Science	Academic Search Premier	RAND Corporation
Science Direct	ACM	Gov.uk
Academic Search Complete	BRIDGE	House of Commons Library
Ingenta Connect	Business Source Complete	Victim Support
APA PsychArticles	Cambridge Scientific Abstracts	Suzy Lamplugh Trust
PubMed	DOAJ	Women's Aid
ASSIA	Economic and Social Research Council	Women's Rights
J-Stor	EDS Archives	Paladin
SCOPUS	Eldis	SafeLives
	FORENSICNetBASE	
	Google Scholar	

Home Office/RDS

Medline

Nexis UK

Social Sciences Citation Index

WorldCat

Study Selection Process

Two research assistants worked independently to identify studies to be included in the review from the above cited databases. In addition, Co-Investigators (Dr Duggan and Dr Franqueira) provided additional relevant sources. The research assistants conducted 35 different search queries and screened over 4,500 articles. After initial screening, 170 articles were deemed relevant and put in relevant folders for each question being examined. 156 of the articles were academic articles and 14 were policy papers. A second stage selection process identified 8 papers that were out of scope or didn't provide trustworthy data so 162 out of 170 articles went through the weight of evidence (WoE) process where 103 were identified for inclusion in this REA, based on methodological criteria set out in Appendix I. All search terminologies used across databases with relevant returns are shown in Table 2.

Table 2. Complete list of terminologies used and relevant results.

Source	Search Terminology	Results (relevant)
Academic Search Complete	(cyber OR digital) AND dating AND (abuse OR violence)	130 (15)
	Digital AND (dating OR partner OR relationship) AND (abuse OR violence)	340 (2)
	Technology AND (abuse OR violence) AND intimate partner	324 (5)
APA PsychArticles	(Digital OR technology OR online) AND (dating OR partner OR relationship) AND (abuse OR violence OR control)	378 (2)
	(Digital OR technology OR online) AND (coercive OR control OR power) AND (partner OR intimate)	40 (0)
ASSIA (Applied Social Sciences Index and Abstracts)	TI(cyber OR techno* OR computer) AND domestic AND (violence OR abus*) NOT child* NOT (Wire Feeds AND Newspapers AND Trade Journals AND Magazines AND Blogs, Podcasts, & Websites AND	587 (5)

	Historical Newspapers AND Other Sources AND reports)	
Ingenta Connect	technology* AND (dating OR partner) AND (abuse OR violen*) AND victim	1 (0)
J-Stor	(ti:((cyber OR digital)) AND ti:((abuse OR violence)))	21 (2)
PubMed	(((technology) OR (digital)) AND (intimate partner)) AND (abuse)	195 (6)
Science Direct	(cyber OR techno OR computer) AND intimate AND partner AND abuse NOT child	794 (12)
	(cyber or online or technology) AND (dating or partner or relationship) AND (abuse or violence or control)	188 (12)
Scopus	TITLE-ABS-KEY (domestic AND abuse OR domestic AND violence OR intimate AND partner AND abuse) AND (online OR cyber OR techno*) not AND child*	226 (0)
	TITLE-ABS-KEY (digital AND dating AND abuse)	49 (16)
	(TITLE-ABS-KEY (revenge AND porn) AND TITLE-ABS-KEY (abuse))	28 (6)
	(TITLE-ABS-KEY (dating AND abuse OR partner AND abuse OR relationship AND abuse OR coercive AND control) AND TITLE-ABS-KEY (digital OR online OR internet OR techno*))	38 (13)
	(TITLE-ABS-KEY (dating AND violence OR partner AND violence) AND TITLE-ABS-KEY (digital OR online) AND TITLE-ABS-KEY (impact))	24 (6)
Web of Science	TS=(Technology Facilitated Domestic Abuse)	23 (16)
	TS=(computer facilitated domestic abuse)	6 (0)
	TS=(cyber* AND abus* AND domestic)	32 (12)
	TS=(online AND domestic AND abuse) NOT TS=child*	124 (5)
	TS=(online AND domestic AND abus*) NOT TS=child*	132 (4) 20 (4)
	TS=(intimate partner violence AND cyber* AND online AND techno*)	25 (3)

	TS=(cyber* AND online AND intimate* AND abus* AND victim*)	64 (5)
	TS=(techno* AND abus* AND victim* AND need*)	167 (0)
	TS=((cyber* OR techno*) AND (abus*) AND (dating*))	33 (0)
	TS=(online AND domestic AND abus* AND impact) NOT TS=child	
Gov.uk	Cyber abuse	88 (1)
House of Commons Library	UK Parliament > House of Commons Library> Home affairs> Crime	461 (3)
RAND Corporation	Research > Cyber and Data Sciences > Cybercrime	200 (1)
Victim Support	"Domestic Cyber Abuse Policy UK"	1
Suzy Lamplugh Trust	"Domestic Cyber Abuse Policy UK"	2
Women's Aid	"Domestic Cyber Abuse Policy UK"	1
Women's Rights	"Domestic Cyber Abuse Policy UK"	1
Paladin	"Domestic Cyber Abuse Policy UK"	1
SafeLives	"Domestic Cyber Abuse Policy UK"	1

Critical Appraisal through Weight of Evidence

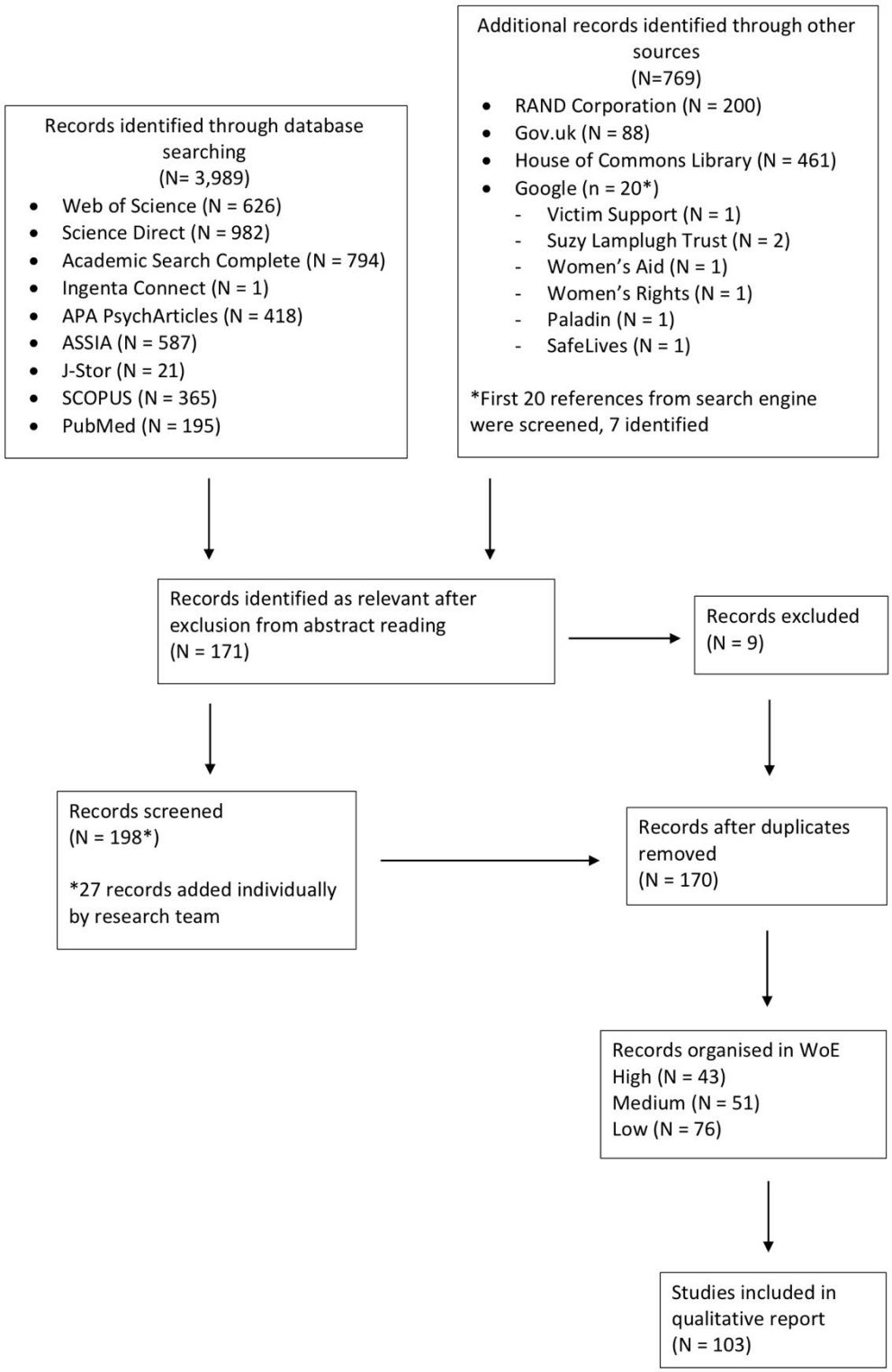
In all reviews of scientific studies, it is important to determine the trustworthiness (i.e., validity and reliability) of sources through an assessment of their methodological appropriateness and relevance to the current review.

The studies yielded from the second stage of the selection process were independently critically appraised for methodological appropriateness and quality (for the full criteria used please see Appendix I). Two reviewers (PI: Dr Afroditi Pina and Co-I: Dr Marian Duggan) worked independently on 3 questions each to apply the weight of evidence ranking to the identified studies (independent WoE spreadsheets can be found in Appendix II). Systematic reviews were included and used where appropriate for context and consolidation of findings.

Overall, the quality of the included studies was mostly medium and some high. As PI Pina and CoI Duggan worked independently in the WoE exercise (PI Pina had questions 1,2,3 and CoI Duggan had questions 4,5,6), the final total of high and low WoE was calculated by removing duplicates and giving the highest WoE attributed to any duplication). Once the agreed manuscripts were given a WoE assessment, PI Pina and CoI Duggan cross checked with each other's questions to ensure relevant information for each was included. Due to their rigour, trustworthiness and relevance to questions, only medium and high WoE papers were

included, with the exception of some low WoE papers that were deemed appropriate for consolidation and context. Additional sources used for context and some literature reviews offering general information were included in the write up but did not go through the WoE process (explaining the discrepancy in the numbers presented in the above tables and the final reference list of this REA). Of the 103 studies included, 43 were graded high in overall trustworthiness in answering some or all the questions of this REA, 51 were graded medium, and 9 were graded low. A bibliographic overview of the medium and high weighted studies included (split by questions) is provided in Appendix III.

Figure 1: Diagram of REA searches and records included in WoE.



MAIN FINDINGS

Working Definition

Technology Facilitated Intimate Partner Violence (TFIPV) is the term agreed by the research team to be the working definition for this REA and we outline it to be any type of abuse (financial, sexual, physical, psychological) and coercive control between current or former intimate partners that is perpetrated or facilitated via technological means, and causes its recipients to experience fear or intimidation, image-based offenses, privacy violation, unwanted sexual attention or physical offenses (Freed et al., 2018; Tanczer et al., 2018; Woodlock, 2017). In the next section we outline the questions set out for this REA and discuss the scholarly definitions and other considerations of IPV facilitated by technology (TFIPV). We highlight a fast-evolving research and policy field and the difficulties associated with accurately and uniformly defining and examining this phenomenon.

What evidence exists about the nature of the different types of TFIPV experienced by adults?

Scholars began to recognise the role of technology in DV and IPV in early 2000. However, from 2010 onwards, TFIPV became a more systematic focus of research in multiple disciplines (e.g., Psychology, Criminology, Law, and Cybersecurity/Computing). One of the seminal studies that fuelled the research and policy focus on technology and its facilitation of IPV was the *SmartSafe* Australian study, conducted by the Domestic Violence Resource Centre Victoria (DVRCV; 2013). This pioneering review of IPV brought together existing knowledge on technology facilitated abuse with the perspectives and experiences of survivors and front-line responders/practitioners. It recognised that, in most cases, stalking was perpetrated by intimate partners or ex-partners, and that the use of technology created an inescapable perpetrator "omnipresence". Domestic violence victims found it difficult to leave the relationship safely, and were often subject to isolation, punishment, and humiliation. The types of technology and online platforms most frequently used by perpetrators to commit TFIPV were smartphones (82%); mobile phones (82%); Facebook (82%); email (52%); and Global Positioning Systems ('GPS') tracking (29%) (Al Alosi, 2017; Harris & Woodlock, 2019; Woodlock, 2017). A substantial proportion of adults who use the internet also use Facebook (80%; Pew Research Centre, 2016) making it the most used Social Networking Site (SNS) and explaining why it features as the most used by perpetrators of TFIPV (Taylor & Xia, 2018).

Definitional Disparities

What became obvious during the searches and synthesising of the available evidence in this report was the multitude of definitions and terms attributed to TFIPV. In their systematic review, Fernet, Lapierre, Hébert and Cousineau (2019) identified the use of a different term for TFIPV in almost all the papers they reviewed (30 terms out of 33 studies). In this REA we

examined 103 individual sources published between 2010 to 2021 and identified 69 different terms (see table 3 for a detailed description of terms and behaviours examined). The lack of definitional consensus indicates a thriving area of research and increasing interest, but also an ongoing debate as to precisely what behaviours and technologies are involved, and whether TFIPV is an extension of IPV or a new form of violence. This lack of consensus also extends to measurements used in studies (over 15 different measurements/scales were identified) to examine the phenomenon, as well as age groups examined, making comparisons between studies difficult, if not impossible (Brown & Hegarty, 2021; Fernet et al., 2019).

Several scholars have expressed concern about the impact of definitional and measurement discrepancy on the interpretation of results and prevalence rates. Studies examining TFIPV use varied methods and measurements, with some studies measuring specific elements such as Image Based Sexual Abuse (IBSA) or cyberstalking and others more broad cyber aggression/controlling behaviours. This can result in widely varied prevalence rates between genders, and these scholars warn that we must consider context regarding the relationship, impact on victim and prominent behaviours to not misinterpret a potential gendered aspect of TFIPV (Douglas, Harris & Dragiewicz, 2019; Dragiewicz et al., 2018; Henry, Flynn & Powell, 2020). In this section we review the available research as well as typologies of available technologies used for perpetrating TFIPV, and the typologies of behaviours enacted using that technology.

Sample Characteristics and Generalisability

Most studies were undertaken with young people and college students, often aged between adolescence (lowest age was 11) and mid-30s. Within these, most participants were female. The sample base adopted by many quantitative (survey-based) studies omitted to examine TFIPV among adults aged over mid-30s. Older people's experiences of TFIPV were represented in qualitative studies, where the purposeful samples were comprised of victims of IPV as opposed to young people and college students. Many of the available studies were conducted in North America, with some conducted in Australia, Canada, Spain, Singapore, Peru, Portugal, and the UK, so non-Western and diaspora populations are less represented. A high proportion of quantitative surveys used one of the existing data capture measures (e.g., Cyber Dating Abuse Questionnaire; CDAQ). These measures have pre-determined statements which respondents indicated whether they had experience of them within the timeframe specified.

Table 3. Terminology used in literature included in this REA, colour coded by WoE

High
Medium
Low

Study	Terminology Used	Forms of Abuse Examined
Duncan & March, 2019	Antisocial Use Of Dating applications	General: enhance perpetrator's? reputations and manipulate social relationships and facilitate sadistic sexual interactions like sending of unsolicited sexual material to matched partners. Esteem: use of Tinder (e.g., for self and other esteem and purposes to self-monitor and promote). Sexual: antisocial sexual behaviour on tinder. Using tinder for sexual and coercive purposes.
Havron et al., 2019	Clinical Computer Security For IPV Victims	Clients expressed a range of chief concerns, 1. Abusers Hacking or having access to client's account. 2. General concerns about abuser tracking them or installing spyware. 3. Few wanted to know more about privacy and had no specific concerns.
Burke et al., 2011	Control of Intimate Partners	Controlling Partners Inventory: 18 controlling or monitoring behaviours towards partners. Checking phones, emails, networking sites, sending excessive texts and emails, and making excessive calls, using GPS to track, passwords, hidden/spy webcams, spyware.
Roundy et al., 2020	Creepware in Interpersonal Attacks	Recognised technology used in creepware. Fake surveillance apps, bomber or repeater text apps, fraud, hack tools etc.
Brem et al., 2019	Cyber Abuse	Cyber abuse entails: sending threatening texts to partner, making threatening calls via mobile phone, monitoring via SNS.

Whitton et al. 2019	Cyber Abuse	Measured cyber abuse in the context of IPV experiences: Cyber Dating Abuse Measure: pressured by partner to send sexual or naked photos, partners writing mean or embarrassing things about victim on SNS.
Schnurr et al., 2013	Cyber Aggression	Dating Relationships Survey: participant victimisation was used as partner perpetration using technology means to perpetrate cyber aggression by embarrassing, controlling, monitoring and arguing.
Crane et al., 2018	Cyber Aggression	Privacy invasion (e.g., checking partner's messages without permission). Cyber relational aggression (e.g., flirting with others on SM for partner to see) that goes beyond traditional IPV.
Mishna et al., 2018	Cyber Aggression	Mixed methods: sharing private photo or video through texts or SNS without permission, sending angry, rude vulgar, threatening messages via text or online, excluding victim from messages or online, impersonating victim, spreading false rumours about victim.
Wolford-Clevenger et al., 2016	Cyber Coercive Control	Partner Cyber Abuse Questionnaire (Hamby, 2013): using victim's social media without permission, embarrassing partner on social media, sending angry/insulting texts, sharing embarrassing texts or pictures of victim, hacking, changing passwords of victims, reading emails without permission, spyware, excessive texts/messages, GPS.
Deans and Bhogal, 2019	Cyber Dating Abuse	Aggression, romantic jealousy, and cyber dating abuse that consisted of Borrajo et al. (2015a,b) measurements of controlling behaviour, monitoring via internet use and mobile technologies and restricting/controlling the internet use of partners.
Borrajo et al., 2015b	Cyber Dating Abuse	Direct aggression, threatening partner or former partner with physical aggression using technologies; control, using mobile devices to monitor and control the internet use or connection of a partner or former partner.
Lara, 2020	Cyber Dating Abuse	Identifies 17 different terms of TFDA.
Branson & March, 2021	Cyber Dating Abuse	Aggressive and controlling behaviours against an intimate partner using technology. Cyber dating abuse is part of IPV/DV, but the perpetrator typologies are claimed to be different.
Villora et al., 2019	Cyber Dating Abuse	Cyber Dating Abuse Questionnaire, 20 items about direct and indirect CDA: threatening partner of using technology to hurt them, or control via mobile applications, monitoring victim use of technology.
Lancaster et al., 2020	Cyber Dating Abuse	Partner Cyber Abuse Questionnaire (Hamby, 2013).

Machimbarrena et al., 2018	Cyber Dating Abuse	Cyber Dating Abuse Questionnaire (Borrajo et al., 2015), sexting Questionnaire (towards partners, friends or strangers), Obsessive Internet Use.
Lu et al., 2018	Cyber Dating Abuse	Cyber Dating Abuse Victimisation: stalked, harassed, controlled, or monitored by a partner online.
Hancock, Keast and Ellis, 2017	Cyber Dating Abuse	14 Cyber Dating Abuse questions (Picard, 2007): threats, humiliation, harsh comments perpetrated by texts, emails, chats, social media.
Van Ouytsel et al., 2016	Cyber Dating Abuse	Cyber Dating Abuse Victimisation scale adapted from the control dimension of the Cyber Dating Abuse Questionnaire (Borrajo et al., 2015a).
Borrajo, et al., 2015a	Cyber Dating Abuse	9 questions developed to assess cyber dating abuse= Cyber Dating Abuse Questionnaire CDAQ): threatening messages, insulting/humiliating messages, posting pictures or messages online to humiliate, spread rumours and gossip about victim, using victim password for monitoring, IBSA, internet/mobile phone used to control monitor history and whereabouts, making victim jealous via contacting ex partners online.
Doucette et al., 2018	Cyber Dating Abuse	Specifically examined the electronic intrusion aspect of CDA: monitoring a partner's SNS, mobile phone and text messages.
Flach & Deslandes,2019	Cyber Dating Abuse	Applications targeting non-consensual monitoring, location tracking, controlling, and spying of ex and current intimate partners.
Duerksen & Woodin, 2019b	Cyber Dating Abuse Victimisation	Victimisation study: Used CARS: threatening messages, harassment on social media, monitoring via social media or accounts or GPS.
van Ouytsel et al., 2016	Cyber Dating Abuse Victimisation	Focused on victimisation by controlling behaviours: emails read without permission, receiving multiple texts and calls, partners using internet to control and monitor whereabouts of victims.

Watkins et al., 2020	Cyber Intimate Partner Aggression	Cyber psychological, stalking, and sexual IPA.
Watkins et al., 2018	Cyber Intimate Partner aggression	Harassment; bullying; threatening; insulting on social media; ignoring; IBSA; pressuring for sexual information, sexting, sextortion; checking email accounts/phones/internet activity; using social media to track partner; GPS tracking; extracting information/images without permission.
Fernet et al., 2019	Cyber Intimate Partner Victimisation	Types: Stalking and control; harassment, sexual cyber intimate partner violence (IPV); indirect sexual cyber IPV; and indirect cyber IPV nonsexual.
Melander & Marganski, 2020	Cyber Intimate Partner Victimisation	Used cyberbullying and cyberstalking measures to create modified scale: partner posted content to taunt victim, hurtful posts, harassment via images (pictures of violence, nudity), shared private photos or videos of victim without consent.
Clevenger & Gilliam, 2020	Cyber Intimate Partner Violence	Chapter: coercion and control, cyberstalking, surveillance, harassment, online sexual victimisation, identity theft.
Pineda et al., 2021	Cyber Intimate Partner Violence (IPV)	Used CDAQ: victimisation and perpetration=direct aggression and monitoring and control.
Lyndon et al., 2011	Cyber Obsessional Pursuit	Cyberstalking; monitoring of ex partners on social media; posting on own social media to taunt ex-partners; asking to be unblocked, creating a false profile; spreading rumours; image-based sexual abuse; writing inappropriate things about ex partners and their social circle.
Taylor & Xia, 2018	Cyber Partner Abuse	Hostility: direct threats. Intrusiveness: monitoring. Humiliation: insulting posts. Exclusion: blocking communication. Direct aggression.
Bui & Pasalich, 2021	Cyber Psychological Abuse	Cyber Psychological Abuse Scale: victimisation and perpetration of psychological abuse via technology: keeping tabs on partner via checking email messages, texts, or inbox messages on SNS, sending materials to embarrass partner etc.
Reed et al., 2019	Cyber Sexual Harassment	Lifetime experience with CSH perpetrated by men assessed by 4 items: pressured to send sexual photos or videos, having sexual photos shared without permission, receiving unwanted/unsolicited sexual photos messages, receiving unwanted emails/messages asking recipient to do something sexual.

Dardis & Gidycz, 2019	Cyber Unwanted Pursuit	Controlling or harassing behaviours via electronic means; GPS/surveillance/threats: use of webcams; hidden cameras; social media to monitor; IBSA; threaten ex-partners; Communication/checking: excessive calls; checking phones/email/web histories.
Charak et al., 2019	Cybervictimisation	Measured by the Cyberaggression in Relationships Scale: psychological aggression, sexual victimisation and stalking also added 2 items on psychological aggression towards LGBT identity (e.g., threats to out, or demands to act straight).
Rothman et al. 2021	Dating Abuse	Used MARSHA=Adolescent Relationship Harassment and Abuse + CADRI. Victimisation and Perpetration by 35 behaviours but Privacy Control was the measurement looking at monitoring through texts/social media/apps looking through partners' phone/social media without permission, demand for passwords or access, excessive messaging to keep track, changed victims' passwords to lock them out of accounts.
Stonard et al., 2017	Dating Violence and Abuse	Qualitative: focus groups Themes: frequency of communication, monitoring and controlling communication, impact of tech assisted abuse compared with in person.
Harris & Woodlock, 2019	Digital Coercive Control	Monitoring and surveillance, public attacks and shaming women, threat of shaming, Women in rural areas more in danger Spacelessness, transcending geography, omnipotence, omnipresence, entrapment.
Woodlock et al., 2020	Digital coercive control	Omnipresence: Technology enabled the perpetrator to invade every aspect of victim's life Isolation and Ostracism: women fear public humiliation (via IBSA) due to threats received by perpetrator and thus result in not using social media and online platforms.
Ellyson et al., 2021	Digital Dating Abuse	Used Reed et al., 2020 DDA victimisation + perpetration scale: digital monitoring and control, digital direct aggression, digital sexual coercion.
Bhogal et al., 2019	Digital Dating Abuse	Digital dating abuse 19 item perpetration subscale. Looking at partners phone, texts social media without permission.

Weathers & Hopson, 2015	Digital Dating Abuse Digital IPA	Qualitative semi structured interviews: experiences with digital dating abuse. Nonassertive assimilation: assuming gracious stance to accommodate needs to perpetrators, averting controversy/conflict with perpetrator. Assertive assimilation: overcompensating, perceiving digital abuse as expression of love. Nonassertive separation: avoiding social media.
Weathers et al., 2019	Digital Dating Abuse	Digital dating abuse was assessed by 10 commonly reported digital dating abuse behaviours: same as Weathers & Hopson.
Reed et al., 2020	Digital Dating Abuse	DDA experiences among Latinx youth (victimisation and perpetration) 36 items. E.g., spread rumours, sent threatening messages, monitoring activity, checking up without permission, engaging in unwanted distribution of sexual images, using social media or mobile devices.
Hinduja and Patchin, 2020	Digital Dating Abuse	5 questions on DDA: looking through contents of phone or other device without permission, preventing victim from accessing mobile or other device.
Reed, Tolman and Ward, 2016	Digital Dating Abuse	Developed 38 measurement of DDA: victimisation, perpetration. Monitoring partner's use of internet and social media, look at confidential information without permission, impersonate victim on social media or phone, spread rumours, threaten to send or sending private material and sexual images/videos, distribute victim information without permission.
Brown, Flood and Hegarty, 2020	Digital Dating Abuse	Perpetration and impact: 38 youth perceptions of DDA (qualitative) Men engage in sexual related behaviours and share nudes. Men and women both engage in controlling behaviours but in diverse ways. Reputation is impacted in men whereas negative emotions are impacted in women. Men misconceive severity on women.
Brown & Hegarty, 2018	Digital Dating Abuse	Review: Identified 16 different instruments measuring DDA. Hostility, aggression, intrusion, humiliation, exclusion, excessive communications, camera/phone non-consensual checking, threatening behaviours, GPS location.
López-Cepero et al., 2018	Digital Intimate Partner Violence	Threats to share information, IBSA, accessing accounts/social networks/phones to control and monitor, sexting, unwanted/disturbing content via email or phone/social media harassment via social media, impersonating, buying things without someone's permission using their account, incessant texting and calling, publishing offensive or false rumours, sextortion, contacting friends and family, demands access to accounts, hacking. Two types of abuse: control-centred and damage centred.
Hellevik, 2019	Digital Intimate Partner Violence and Abuse	Harassment: humiliation, negative comments, spreading rumours, constantly messaging, or calling, threatening. Control: blocking friends, pressuring victim to block friends, calling victim's friends to gather information, contacting new partner of victim to sabotage, deleting victims SNS profiles posts, threatening.

		Monitoring: making fake accounts and adding victim, making requests, contacting friends and family of victim, checking victim's social media activity, checking victim's phone. Sexual coercion: pressuring victim to send intimate images, redistributing intimate images, threatening in person physical sexual violence.
Kellerman et al., 2013	Electronic Aggression	Bullying/Harassment/Threat through electronic communication. Image-based sexual abuse (IBSA). Intrusive calls or texts to monitor. Fake profiles/hacking.
Reed et al., 2015	Electronic Intrusion	Using social media to invade the privacy of a partner, and monitor whereabouts and activities; monitoring partner's whereabouts using phone without permission.
Parsons et al., 2017	Gendered Surveillance Stalkerware	Spyware that is explicitly sold or licenced to facilitate intimate partner violence, abuse, or harassment, including pernicious intrusions into the targeted person's life by way of physical or digital actions. Spyware can also operate as stalkerware (e.g., monitoring young children or employees) is repurposed to facilitate intimate partner violence, abuse, or harassment.
Dimond, Fiesler and Bruckman, 2011	ICT and Domestic Abuse	Interviews of women in domestic violence shelters: sending death threats via emails/texts, spreading rumours, sending threats to family and friends of victim, having to go offline and lose connection to family and friends to avoid the perpetrator, harassment on SNS, SNS used as extensions of abuse, using GPS technology.
Henry & Flynn 2020	Image Based Sexual Abuse (IBSA)	Chapter: feminist critique. IBSA= non-consensual recording of sensitive sexual/private material, sharing of intimate material without permission, threats to share intimate material.
Vitis, 2020	Image-based Sexual Abuse	Sextortion, NDII, sexual voyeurism. Threats or actions of sending content to family members or acquaintances.
Henry, Flynn and Powell, 2018	Image-based Sexual Abuse (IBSA)	Interviews with stakeholders and experts/police. Nonconsensual taking/creating, nonconsensual sharing/distribution, threats to create or share intimate images.
Melander, 2010	Intimate Partner Cyber Harassment	Situational couple violence (SCV) Intimate terrorism (IT). Mutual Violent Control (MVC), both partners exert control using technology. Violent Resistance (VR), retaliation towards an aggressive partner via technology. Omnipresence, 'always in your inbox'. Secondary victimisation.

Trujillo et al., 2020	Intimate Partner Cyber Victimisation	Cyber Aggression in Relationships Scale (CARS): psychological abuse, sexual abuse, specific LGB identity cyber aggression and cyberstalking.
Smoker & March, 2017	Intimate Partner Cyberstalking	Cyberstalking: overt vs covert assessed by the Intimate Partner Cyberstalking Scale IPCS: monitoring partner through social media, tracking partner through GPS or applications, going through partner's phone or emails.
March et al., 2020	Intimate Partner Cyberstalking	Controlling relationship behaviours e.g., trying to make someone jealous and intimate partner cyberstalking assessed by the IPCS.
Cantu & Charak, 2020	Intimate Partner Cybervictimisation (IPV)	Cyber IPV measured by the CARS but adapted for victimisation: psychological cyber IPV=receiving harassing/threatening messages from partners via phone, text, SNS. Sexual Cyber-IPV= threatened or suffered sending intimate, naked or sexual photos. Cyberstalking= partner checked phone to see communications
Chatterjee et al., 2018	Intimate Partner Spying (IPS)	Personal tracking (e.g., location tracking, remote locking, syncing SMS, call log and browser history); Mutual tracking (e.g., mutual location sharing, family tracker, alerts of friends in vicinity); and subordinate tracking (e.g., employee tracking, parental controls, and overt and surreptitious spying).
Bellini et al., 2021	Intimate Partner Surveillance	Looked at narratives of IPS from perpetrators, included cases where poster introduced themselves, their target, and other people, described a single or pattern of events and signified motivation in bringing about change.
Wood et al., 2020	Intimate Partner Violence	IPV in higher education institutions. Measured cyber violence victimisation from 8 questions of the CADS.
Leitão, 2018	Intimate Partner Violence (IPV) Digital Technologies and cyber-aggression And Cyber-harassment	Harassment through instant messaging is the most common type of technology enabled abuse.
Tanczer et al., 2018	IoT Technological Abuse	Threats and abuse perpetrated by IoT and smart home devices.
Parkin et al., 2019	IoT Facilitated Tech Abuse	Threats perpetrated via and IoT ecosystem: wearable devices that allow perpetrators to monitor, phones that could provide perpetrators with access, laptops and tablets that perpetrators can change settings, remote control of heating, lighting and blinds, audio and video recording via security cameras and TVs and smart security.

Laxton, 2014	Online Abuse and Domestic Violence	Women's Aid report: abuse through SNS, harassment, abuse, stalking from ex-partner online.
Caridade, Pedrosa e Sousa and Dinis, 2020	Online Dating Abuse	CDAQ used translated in Portuguese victimisation and perpetration.
Gracia-Leiva et al., 2020	Online Dating Violence	CDAQ to measure cyber dating abuse: direct aggression (sending and/or uploading intimate images or videos with sexual content without permission) and control and monitoring (checking mobile devices and SNS accounts without permission).
Grimani et al., 2020	Online IPV	Monitoring, interpersonal electronic surveillance, cyberstalking, intrusive behaviours, harassment, unauthorised access and altering of information for victim.
Brem et al., 2015	Online Mate Retention Tactics	Facebook mate-retention tactics, Facebook jealousy, Facebook surveillance, intimate partner violence. Jealousy and surveillance, and punishment of infidelity items (e.g., check status of partner on FB to check where they are, ask to be given FB passwords, monitor partners FB chat and messages, threaten with break up if someone.
Melander & Hughes, 2018	Partner Cyber Aggression	Persistent unwanted text or online messages, posting private information, photos, or videos without permission.
Levy & Schneier, 2021	Privacy Threats In Intimate Relationships	intimate threats, snooping around without permission, using ownership of devices to monitor and control, use knowledge of victim to gain access to accounts and passwords.
Ross et al., 2019	Sexting Coercion	Sexting coercion: persistent requests to send or produce intimate images and videos and communicate in a sexualised manner via text messages and emails.
Drouin et al., 2015	Sexting: Digital Intimate Partner Aggression	Sexting coercion IPV.
Harkin et al., 2020	Spyware And Intimate Partner Abuse (IPA)	The general deployment of spyware: a) is often utilized in forms of intimate partner abuse: b) is "morally troubling" from the perspective of being corrosive to many forms of social relations (Loader et al., 2014: 469); and c) has limited contexts where it could be deployed without violating surveillance laws.
Freed et al., 2018	Stalking/Domestic Abuse And Technology	**Ownership based access:** exploiting legal ownership of victims' devices or online accounts. They can physically prevent victim from use of device or account, turn off the internet, and track location and monitor usage via family plans etc.

		Account/device compromise: compromise victims' accounts by guessing their passwords or forcing them to disclose them. hack security passwords and questions remotely, install spyware, monitor through IoT, monitor via SNS text or email, steal information such as bank accounts, delete victim's data, change victim's password so locking them out of accounts and impersonate victims. **Harmful messages/posts:** Call/text/message from identifiable or anonymised accounts (e.g., spoofed number or fake SNS profile), post content to humiliate victim or threaten, harass victim's friends and family, facilitate harassment of third parties (abuser's new intimate partner). **Exposure of private information:** Threaten to expose information to blackmail victim, posting private information (doxing) about victim (e.g., medical status), revenge porn/IBSA, Create fake profiles advertising sexual services of victim.
Lopez-Neira et al (2019)	Tech Abuse and Internet of Things (IoT)	Internet connected devices at shared home spaces used to intimidate, gaslight, harass and monitor victims.
Duerksen & Woodin, 2019a	Technological Intimate Partner Violence (tIPV)	Social media use. Technological disinhibition.
Tseng et al., 2021	Technology Enabled IPV	Perpetrators use standard interfaces to abuse. Remote attacks through disclosing sensitive information, unsolicited contact, repurposing common apps as spyware. Online infidelity forums are instrumental in abusers learning how to abuse.
Woodlock, 2017	Technology Facilitated Abuse	Stalking: text messaging, tracking location, accessed devices without permission, IBSA, co-occurs with emotional abuse, sexual abuse, physical violence, and financial abuse. *Omnipresence.* Isolation: Direct harassment of friends and family via texts phone and social media. Indirect harassment: having to change phone numbers, relocate or go offline to avoid perpetrators. Punishment/Humiliation/IBSA: either threat or actual public setting embarrassment for victims via social media.
Brown & Hegarty, 2021	Technology Facilitated Abuse In Relationships (TAR)	Humiliation, Monitoring and Control, Sexual Coercion, and Threats.
Al-Alosi, 2017	Technology Facilitated Abuse/Cyber Violence/Digital Abuse	GPS tracking and sat nav technology, spyware applications (software developed for other purposes), surveillance cameras, keylogging (recording keystrokes on computer). Social media (Facebook in particular), monitoring, hacking, publicly harassing, false accounts, impersonating Emails, texts, phone calls, bypassing protection orders. Revenge porn/IBSA.

Dragiewicz et al., 2018	Technology Facilitated Coercive Control	Review. Abuse and harassment online via social media by partners and ex intimates, image based sexual abuse, misogynist networks cyber mobbing, doxing.
Yardley, 2020	Technology Facilitated Domestic Abuse	Using mobile phones, SNS and GPS to track and monitor victims. Omnipresence (inescapable perpetrators and abuse due to technology) covert, overt and retributive.
Douglas, Harris and Dragiewicz, 2019	Technology Facilitated Domestic and Family Violence	Interviews: isolation, monitoring and stalking, IBSA, social media abuse (Facebook), harassment
Henry et al, 2020	Technology Facilitated Domestic And Sexual Violence	**Digital dating abuse** (IBSA, password access, surveillance and monitoring, constant communication/harassment). **Intimate partner cyberstalking** (repeated threats or harassment via digital communication which cause the victim to feel afraid; gathering information, impersonation, computer hacking, false accusations, repeated contact/harassment, monitoring intimidation and threat via phone/sms/calls computer, SNS, GPS, Drone etc.). **Technology facilitated sexual assault** (technology used by predators to meet victims on dating sites to sexually assault, rape-by-proxy (posting messages online calling third parties to assault a victim or pretending to be a victim) coercing victims into engaging in sexual acts or sending images (sextortion). **Image based sexual abuse:** creating and distributing intimate images of a person without their consent. Can be hacked, or shared, videos, images or deepfakes. **Online Sexual Harassment:** Unwanted sexual attention, requests for dates, requests for sex, simulated rape, cyberflashing.
Leitão, 2019b	Technology Facilitated Intimate Partner Abuse	Coercive control and gaslighting via digital technologies. Monitored devices and accounts, hijacked, or hacked accounts and devices, spyware and covert monitoring, non-consensual sharing of intimate images and outing.
Leitão, 2019a	Technology Facilitated Intimate Partner Abuse	overt and covert surveillance, physical restrictions to devices, threats of harassment and abuse, evidence gathering, social media used by victims for support.
Zhong et al., 2020	Technology Facilitated Sexual Violence	Online sexual harassment, image-based sexual exploitation, cyberstalking, gender- and sexuality-based harassment, and sexual assault and/or coercion.

Powell & Henry, 2019	Technology Facilitated Sexual Violence Victimisation (TFSV)	Negative online behaviours and hate speech + TFSV victimisation scale: digital harassment, IBSA, sexual aggression/coercion, gender/sexuality-based hate speech.
Eterovic-Soric et al., 2017	Technology Used By Stalkers	Review: stalking and surveillance facilitated by technology. GPS trackers, spyware, keyloggers, smartphones and SNS, IBSA.
Messing et al., 2020	Technology-based Abuse	Measured by two questions on monitoring: interactions with others via SNS or technology, tracking whereabouts via SNS or technology. Cyberstalking, harassment online and monitoring: impersonation, watching, staking, threatening.
Freed et al., 2019	Technology-enabled IPV	Technology Assessment Questionnaire (TAQ) devised to assess victim vulnerabilities: how victims choose their passwords, whether abuser knows information, questions about SNS settings, mobile phones, family plans and child devices.
Harkin & Molnar, 2020	Technology-facilitated Abuse	Consumer spyware. Jail-breaking mobile devices, more often Android than iPhone. Gender-based abuse
Gilchrist et al., 2017	Technology-facilitated Abuse	Controlling behaviours , TFA.
Alshehri et al., 2020	Technology-facilitated Abuse	Tech abuse: any abuse using technologies such as smartphones, personal computers, or social media. Smart Home Facilitated Tech Abuse (SHOT): using smart home devices.
Powell and Henry, 2018	Technology-facilitated Sexual Abuse (TFSA)	Indirect forms of harassment, i.e., sharing unpleasant memes. Tracking down CSA victims as adults and harassing them about their CSA experiences.
Hertlein et al., 2020	Technology-mediated Intimate Partner Violence (IPV)	Technology to exert control, monitoring, putting someone down, unwanted invasion of privacy, sexual threats online, coercive messages, spreading rumours, IBSA, sexting.

Technologies Used in TFIPV

The literature on technologies utilised in the perpetration of TFIPV is rapidly growing. As technology is evolving at great speed, research examining this phenomenon is catching up. Researchers from multiple disciplines (e.g., Psychology, Sociology, Criminology, Law, Cybersecurity, Digital Systems, Telecommunications, Engineering) are coming together to identify and assess available technologies and the risks associated with them (see Figure 2 for a breakdown of technologies used by stalkers identified by Eterovic-Soric et al. in 2017). There are two main types of technologies recognised by most scholars in the field: Technologies marketed specifically for control, surveillance and harassment [e.g., spyware, stalkerware, text repeaters (online tools allowing for the repetition and sending of a text multiple times)] that are downloaded and installed by perpetrators, and technologies not marketed as such, but repurposed by perpetrators to exert monitoring, control, and manipulation (e.g., dual use technologies; baby monitors, smart devices, phone locators, social media platforms) (Chatterjee et al., 2018; Fernet et al., 2019; Havron et al., 2019; Parsons et al., 2019; Roundy et al., 2020).

Freed et al. (2019) identified attackers with intimate knowledge of victims (e.g., former or current partners) as the most difficult type of cybersecurity threat, and one that conventional threat models and countermeasures do not adequately anticipate or address. The attacks are considered "technologically unsophisticated" in cybersecurity terms because they are carried out by an authenticated user that interacts with victims' devices or systems via standard interfaces. They identified two main technology modes that intimate partner perpetrators can attack victims: *ownership-based access* and *account/device compromise*. Abusers frequently exploit their legal ownership of victims' devices or online accounts, whereby they can prevent victims from using these devices/accounts, turn off their internet access, track their location, monitor their usage via family plans and so forth. They can also compromise victims' accounts by guessing or forcing victims to disclose passwords, stealing information, impersonating victims, and downloading and installing spyware/stalkerware.

Flach and Deslandes (2019) identified over 200 applications with stalkerware features and 40 applications specifically marketed towards intimate partner spying, control, and tracking. Chatterjee et al. (2018) searched combined web and app stores with query recommendation Application Programming Interfaces (API) and identified over 600 queries for spyware apps and 200 apps over the space of one month. The applications were classified into three categories based on their capabilities: *personal tracking* (e.g., location tracking, remote locking, synchronizing Short Messaging Service (SMS; text messages), call log and browser history), *mutual tracking* (e.g., mutual location sharing, family tracker, alerts of friends in vicinity) and *subordinate tracking* (e.g., employee tracking, parental controls, and overt and surreptitious spying). Importantly, Parsons et al. (2019) found that spyware companies had extensive references to spousal monitoring in their optimisation content and favoured terms that identified the use of tools for spying. Harkin et al. (2020) also highlighted the commodification of spyware, the marketing messages that appear in support of non-consensual use, and the responsibility of app developers in the proliferation of TFIPV.

In their report examining the installation of stalkerware on mobile phones and potential victims of stalkerware during 2019, the Kaspersky Security Network (2020) placed the Russian

Federation in 1st place worldwide with 23.4% of users affected, Brazil came in second place with 9.4% of users affected and India in 3rd with 9%. The US holds fourth place with 5.6% and the UK holds the 8th place globally with 1.95% (Kaspersky Security Network, 2020). However, these statistics do not paint a full picture as these are numbers collected by this institute based on its own product which alerts users to the presence of spyware/stalkerware on their (Android) phones. Therefore, there is missing data from users of other types of phone interfaces and those who do not have this alert. Despite stalkerware being overall less prevalent than other technological attacks—such as malware and adware—the Kaspersky Security Network (2020) highlight that illegal surveillance malware is on the decline, whereas stalkerware is fast becoming a rising and significant factor in the cybersecurity landscape. Its potential impact and risk for victims may be much more impactful, since it is technology used by people who target specific individuals and is linked with other types of abuse (physical and psychological).

While social networking sites have garnered increasing recognition, security risks in devices such as laptops, phones, technologies marketed specifically for control and surveillance, and insidious or repurposed technologies, pose new challenges for scholars and policy makers alike (Leitao, 2019a; Lopez-Neira, Patel, Parkin, Danezis & Tanczer, 2019; Tanczer, Lopez-Neira, Parkin, Patel & Danezis (2018). The Internet of Things (IoT) is a term used to describe the fast-evolving technological terrain encompassing a gamut of devices that have the capability of communicating with each other (e.g., smart household appliances like Amazon's Alexa and Echo, Google Home, wearable devices, Nest thermostats, fridges, cameras, smart security, doorbells etc). These technologies have been recently linked with the perpetration of TFIPV and in particular stalking, monitoring and controlling victims, with some researchers proposing that these technologies are less risky and more effective for perpetrators (Lopez-Neira et al., 2019). These are normally perpetrator-owned devices and shared with the victims in a home setting where the perpetrator can access them physically and remotely, controlling ambient surroundings and insidiously monitoring or gaslighting victims (e.g., by locking and unlocking doors remotely, triggering alarms, changing heating settings, etc.) (Alshehri, Ben Salem & Ding, 2020; Leitao 2019b; Parkin et al., 2019).

Figure 2: Eterovic-Soric et al., (2017, p.282) summary of technologies used by stalkers.

Table 1 – Summary of technologies used by stalkers.

Technology	Monitoring	Tracking	Harassment	Impersonation
GPS trackers		Yes		
Keyloggers	Yes			
Hidden cameras	Yes			
Webcams	Yes			
Audio bugs	Yes			
Long-range microphones	Yes			
Telephones/VoIP			Yes	
Location-based dating apps		Yes	Yes	
Spyware	Yes		Yes	
Mobile stalker apps	Yes	Yes	Yes	Yes
Online email accounts	Yes		Yes	Yes
Social media	Yes		Yes	Yes
Marauders Map		Yes		
Reverse image search tools	Yes			
Human flesh search engines	Yes		Yes	
Bluetooth/AirDrop			Yes	
Distributed Denial of Service			Yes	
Email/chat			Yes	
Non-consensual pornography websites			Yes	

Types of TFIPV Behaviours

In 2014, the US National Network to End Domestic Violence identified 6 different prominent categories in which technology is used to perpetrate IPV: monitoring; harassment; impersonation; tracking/stalking; Image Based Sexual Abuse (sharing or threatening to share intimate images of a current or former partner); and abusing children's technology. The latter category included using technology given to children (such as laptops and mobile devices) or monitoring their social media to spy on a current or former partner (Eterovic-Soric et al., 2017). Several attempts at creating classifications and typologies have followed since, based on motivation, mental health and type of harmful behaviour. This has coincided with debates around whether TFIPV is another manifestation or extension of IPV or whether it should be seen as a separate type of abuse. Overall, most experts maintain that TFIPV is an extension of IPV and hence, needs to be classified in typologies allied to offline abuse (e.g., sexual, verbal/emotional, physical). For this section we focused on the nature of the behaviour to denote different types of TFIPV (e.g., Fernet et al., 2019).

The diverse nature of TFIPV experienced by young people and adults spanned a range of types, across direct and indirect means. Some were public, others private. Some were a violation of the victim's privacy, some not. Some were focused on controlling the victim and others on damaging the victim's reputation. The abuse also tends to be multimodal, with patterns of behaviours presenting simultaneously (e.g., monitoring as well as harassing texts, etc.; Freed et al., 2019) For the purposes of this review, TFIPV can be summarised, based on behaviours identified, in four main types and two modes. The types are: *Cyberstalking and Coercive Control, Harassment, Image Based Sexual Abuse,* and *Indirect Non-Sexual Abuse* (Al-Alosi, 2017; Dardis & Gidycz, 2019; Henry et al., 2020; Kellerman et al., 2013; Lopez-Cepero et al., 2018; Lyndon, et al, 2011; Reed et al., 2015; Watkins et al., 2018). The modes are: *Direct* (e.g., using technology to harass and intimidate a victim directly) and *Indirect* (e.g., using technology or social networking platforms to comment about the victim in a public or social setting) (Kellerman et al., 2013; Lyndon et al., 2011; Fernet et al., 2019).

Cyberstalking and Coercive Control:

Controlling behaviours and surveillance (alongside harassment via instant messages) were the most frequently reported types of TFIPV in the literature reviewed. Some types of monitoring and control can be found frequently even in non-abusive relationships and are often considered as legitimate responses to perceived or real extradyadic threats (e.g., checking partner's phones/SNS accounts; Borrajo et al., 2015b; Brem et al., 2015; Grimani, Gavine & Moncur, 2020; Leitao, 2018; 2019b). Surveys in Australia, the US and the UK all reported that victims had experienced TFIPV using location technology and surveillance tactics (Levy & Schneier, 2020; NPR, 2021; Pew Research Centre 2017; Women's Aid, 2020;). These behaviours include: tracking the location of the victim via GPS technology or SNS, hacking, accessing devices without permission, monitoring victims' last mobile phone connection, using victims' personal passwords, checking victims' emails and messages without authorisation, keystroke and login hardware, creating fake profiles on SNS to monitor and track the communications of current or ex partners, and installing tracking and monitoring applications (e.g. spyware or stalkerware) without the victim's knowledge or permission (Al Alosi, 2017; Borrajo et al., 2015a; Chatterjee et al., 2018; Douglas, Harris and Dragiewicz, 2019; Freed et al., 2019; Levy & Schneier, 2020; Lyndon et al., 2011; Reed et al., 2015; Taylor & Xia, 2018; Watkins et al., 2018; Woodlock 2017). Despite these being featured in the harassment category, repeated threats and insults via email, calls or text messages or other technology mediated communication are cyberstalking behaviours and therefore need to be part of this type too (Dardis & Gidycz, 2019; Henry, Flynn & Powell, 2020; Smoker & March, 2017; Watkins et al., 2018).

Harassment:

This is an umbrella term that includes *direct* (e.g., targeting the victim) sexual and non-sexual behaviours perpetrated via technology in a public or private setting. Excessive/harmful calls to the victim and text messages via instant messenger applications and social media (e.g., Whatsapp, Facebook Messenger, Instagram and Twitter via Direct Messages) and pressures for sexual information or sexualised conversation (e.g., sexting) were encountered in the majority of studies examining TFIPV (Borrajo et al., 2015a; 2015b; Drouin et al., 2015; Freed et al., 2019; Kellerman et al., 2013; Leitao, 2018; Ross et al., 2019; Watkins et al., 2018; Woodlock, 2017). Uploading content and complaining about the victim via stories, threads or posts, spreading rumours and creating false profiles on SNS or blogs with the intent to cause humiliation, (Kellerman et al., 2013; Lyndon et al., 2011; López-Cepero et al., 2018; Melander, 2010; Watkins et al., 2018; Woodlock, 2017), posting private information (doxxing) about a victim (e.g., immigration status/medical information), exclusion from online fora, subscribing the victim to services without consent and disruption of a victim's email flow were some additional harassing behaviours identified (Fernet et al., 2019; Freed et al., 2018; Levy & Schneier, 2021).

Image Based Sexual Abuse:

This is an umbrella term that encompasses direct and indirect behaviours that constellate around private/sexual material that is shared with others without consent. This material can be obtained *directly* from the victim via pressure/force, or consensually during the relationship, and *indirectly*, via hacking computers, mobile phones or IoT devices, or physically

getting access into victims' devices without permission. Behaviours identified in the literature included the distribution of sexual images or videos, making threats to distribute said material, blackmailing and pressuring victims to obtain further images/material, sending the victim intimate sexual images without consent, and making threats to expose information to blackmail or control a victim. In some cases, TFIPV included enlisting third parties in the harassment of victims by creating fake dating profiles and rape-by-proxy where perpetrators were advertising sexual services of victim thus enlisting third parties in the potential assault of victims (e.g., Dardis & Gydicz, 2019; Henry, Flynn & Powell, 2020; Kellerman et al., 2013; Leitao, 2018; 2019b; Lyndon et al., 2011; Vitis, 2020; Watkins et al., 2018).

Indirect Non-Sexual Abuse:

These behaviours involve indirect harassment of a victim, via the victim's new partner, family, friends and acquaintances, third party harassment where abusers enlist other users in the harassment of victims (e.g., vigilantism), and posting fake information online for services offered by victims (e.g., items for sale where people would contact the victim to buy) (López-Cepero et al., 2018; Woodlock, 2017; Woodlock et al., 2020).

Who are the perpetrators of TFIPV?

Most studies drew their sample of perpetrators from a population base of students and young people, with the inclusion criteria requiring survey participants to be, or recently have been, in a romantic relationship. As a result, many studies noted the early age from which these behaviours begin and the need for similarly early interventions (for both victims and perpetrators).

There was variability between studies which indicated whether perpetrators of TFIPV were also likely to engage in offline IPV. Some indicated that perpetrators limited their activities to online means only (Melander and Hughes, 2018) while others demonstrated engagement in both online and offline abuse (Brem et al., 2019; Bui & Pasalich, 2021; Caridade et al., 2020; Lara, 2020; Lyndon et al., 2011; Watkins et al., 2020).

Studies exploring the factors associated with perpetration highlighted the presence of jealousy (Branson and March, 2021; Borrajo et al., 2015b; Dardis & Gidycz, 2019; Deans and Bhogal, 2019; Ellyson et al., 2021; Flach & Deslandes, 2017; Kellerman et al., 2013; Watkins et al., 2018); anger or hostility (Deans and Bhogal, 2019; Ellyson et al., 2021; Kellerman et al., 2013; Watkins et al., 2018); alcohol consumption/substance abuse (Brem et al., 2019; Crane et al., 2018; Duerksen & Woodin, 2019a; Watkins et al., 2020); attachment anxiety, deficits in self-regulation (Dardis & Gidycz, 2019; Reed et al., 2020); and social media use (Brem et al., 2019; Duerksen & Woodin 2019b; Melander, 2010). This latter category alludes to SNS providing particularly conducive environments for controlling, monitoring and inflammatory behaviours in intimate relationships. Zhong, Kebbell and Webster (2020) examined the concept of toxic online disinhibition (also linked to cyberbullying) whereby communication via online or computer means disinhibits certain individuals in perpetrating negative behaviours (e.g., offensive language, trolling, harassment) because they perceive the online arena as something separate from offline communications, and mostly free of sanctions (also

found in Duerksen & Woodin, 2019b, Hellevik, 2019 & Melander, 2010). Zhong et al., (2020) in their study with university students found that prominent levels of toxic disinhibition and prior sexual aggression towards a partner would predict an increased likelihood of TFIPV perpetration.

Gilchrist, Canfield, Radcliffe & D'Oliveira (2017) examined men receiving substance abuse treatment in England and Brazil and found that the majority had reported controlling behaviours in their most recent relationship, while a similar percentage also reported TFIPV (33% and 30% respectively). Controlling behaviours were related with adverse childhood experiences, anger and severe physical IPV perpetration, while TFIPV perpetration was associated with being of a younger age and also having experienced TFIPV from a partner.

Many studies suggested that gender was not a significant predictive factor for victimisation or perpetration (e.g., Bui & Pasalich, 2021; Dardis & Gidycz, 2019; Reed et al., 2015) but gender variation in the nature of the perpetration is reported in some studies (Branson & March, 2021; Borrajo et al., 2015a, 2015b; Dardis & Gidycz, 2019; March et al., 2020). TFIPV perpetrated by males was considered more overt (conducted publicly), direct and severe than TFIPV perpetrated by females, while females were more likely to engage in controlling behaviours (e.g., monitoring a partner's social media and phone) (Brown, Flood and Hegarty, 2020; Dardis & Gidycz, 2019; Pineda et al., 2021; Smoker & March, 2017). Furthermore, males and females engage in different forms of antisocial use of dating apps (e.g., Tinder); females are more likely to use dating apps for self and other esteem purposes and self-promotion whereas males are more likely to use dating apps for antisocial sexual/predatory behaviours (e.g., sending unsolicited sexual imagery and coercing matches into sexual behaviour online; Duncan & March 2019). Similarly, Kellerman et al. (2013) found that motivations for TFIPV perpetration differ between genders, with men likely to perpetrate it due to insecurity, humour, negative emotions and retaliation, whereas women additionally reported motivations such as jealousy and privacy reasons.

Dardis and Gidycz (2019) found that women were more likely to engage in minor cyber unwanted pursuit behaviours (CUPB) than men, whereas there was no gender difference in the prevalence of severe CUPB. According to the authors, minor CUPBs are set apart by reconciliation or romantic motives whereas severe CUPBs are underscored by retaliation and control motives.

Some studies have used established measurement scales which incorporated questions assessing for bidirectionality of TFIPV (one individual experiencing victimisation and perpetrating TFIPV) (Brem et al., 2019; Reed, Tolman and Ward, 2016; Melander and Hughes, 2018; Rothman et al., 2021) finding that cyber aggression perpetration in intimate relationships has a bi-directional and dyadic nature and can be perpetrated by all genders (e.g., to embarrass, argue with, control, and monitor a partner). Relatedly, Brem et al. (2019) found that 84% of perpetrators of TFIPV were also victims of cyber abuse. Schnurr, Mahatmya, and Basche (2013) found that elevated levels of online aggression from female partners decreased men's physical IPV perpetration. According to the authors, online victimisation from female partners resulted in weakened reactions and lesser IPV perpetration, whereas men who were subjected to more subtle TFIPV by female partners were more likely to perpetrate IPV.

Similarly, Brown, Flood and Hegarty (2020) found some males indicated a positive impact (for themselves) when engaging in TFIPV, particularly when involving the distribution or collection of (non-consensual) nude images of females. Males in their sample failed to recognise the fear that women may feel if subjected to this, instead suggesting that they might feel flattered or were able to challenge such behaviour if unhappy. Furthermore, Bhogal et al. (2019) examined TFIPV, especially digital dating abuse as a mate retention tactic (also see Brem et al., 2015 who found a link between Facebook mate retention tactics and aggression in relationships), where those who considered their partner to be of higher mate value to them (e.g., more attractive) were more prone to perpetrate TFIPV. Borrajo, Gámez-Cuadix and Calvette (2015b) found that individuals who were more likely to endorse erroneous beliefs/myths about love (e.g., jealousy is proof of love) were more likely to exert control via TFIPV in relationships. They also found that justification of TFIPV (e.g., it is acceptable to spread rumours about a partner if they transgressed) and perpetration of direct aggression was stronger in younger women in that sample.

Personality traits and mental health correlates have been examined in a limited number of studies, with findings indicating that Dark Tetrad personality traits (e.g., Machiavellianism, Narcissism, Psychopathy and Sadism) and attachment anxiety are linked with perpetration of TFIPV and other online aggressive behaviours (Branson & March, 2021; Bui & Pasalich, 2021; Duncan & March, 2019; March et al., 2020; Pineda et al., 2021; Reed et al., 2015; Smoker & March, 2017). Bui and Pasalich (2021) found that attachment anxiety (e.g., anxiety about relationship with significant others), borderline personality disorder traits (such as mood swings, shifting self-image, fear of abandonment) and psychopathy traits were associated with more frequent perpetration of TFIPV as well as offline DA/IPV. Pineda et al. (2021) also found positive associations between psychopathy and narcissism with cyber controlling behaviours and psychopathy being associated with direct cyber aggression behaviours (consistent with the aggressive nature of people high in psychopathic traits). TFIPV perpetrators presented with higher overall dark personality traits and gender-based differences than offline IPV/DA perpetrators. Gender differences in personality traits and links to TFIPV have also been highlighted by studies; females are more likely to self-report Machiavellian traits whereas males are more likely to report Machiavellianism, psychopathy, and sadism (Duncan & March, 2019).

What are the vulnerabilities and needs of TFIPV victims?

Most of the research on victimisation is focused on adolescents, with some addressing young/emerging adults. When the mean age of the sample was below 18 years, or when we could not decipher the vulnerabilities and needs of adults (younger or older), the research was excluded from consideration. Some research which focused on adolescents, however, is mentioned for context throughout this report. Overall, the most consistent finding is that experiencing offline IPV is the most predictive vulnerability factor for TFIPV (Borrajo et al., 2015a; Duerksen & Woodin, 2019a; Fernet et al., 2019 Marganski & Melander, 2015; Taylor & Xia, 2018). It is useful to note that it is difficult to glean whether TFIPV vulnerabilities and needs are specifically related to the online format, or whether it is due to victims being in an abusive relationship overall and TFIPV is just another manifestation of that abuse.

Literature on TFIPV victimisation among adolescents and young adults shows a significant link with negative mental health outcomes and psychosocial functioning (e.g., lack of social support, lower quality of life, PTSD, depression), and maladaptive coping strategies such as alcohol and substance use, risky sexual behaviours (e.g., younger onset of sexual activity and with multiple partners), antisocial behaviour, suicidal ideation and suicide risk (Cantu & Charak, 2020; Duerksen & Woodin, 2019b; Lu et al., 2018; Melander & Marganski, 2020; Reed, Tolman & Ward, 2016; van Ouytsel et al., 2020).

Overall, women of younger and older ages are more likely to report greater impacts, as well as risks of TFIPV, than men; Gracia-Leiva et al. (2020) found that being young, a female and having experienced both offline and online dating violence carries a tenfold increase of suicide risk. Suicide risk was only reduced with the presence of peer and parent proximity, and in particular for those young adults who could confidently communicate with their peers. Ross et al. (2019) reported that sexting coercion was more likely to be experienced by women than men, and that it was significantly and independently linked to negative mental health problems and attachment dysfunction. Additionally, Lancaster et al. (2020) identified individuals who had experienced TFIPV, also reporting higher attachment avoidance (e.g., less seeking of closeness or expressing emotion). Pineda et al. (2021) also highlighted that dark personality traits such as Machiavellianism, narcissism, and sadism are linked with TFIPV victimisation (in parallel to perpetration).

Some studies indicated additional vulnerabilities for victims with disabilities, as well as culturally and linguistically diverse victims (Douglas, Harris and Dragiewicz, 2019; Woodlock et al., 2020). Disabled victims are at increased risk as they rely on technology to access services or to communicate (e.g., hearing impaired victims relying on phones to text) that may be restricted by the perpetrator. Learning disabled victims are also at increased risk, particularly of IBSA as well as TFIPV via financial control (Douglas, Harris, & Dragiewicz, 2019). Linguistically and culturally diverse individuals are also at increased risk due to perpetrators' limiting their use of technology to connect with friends and family. In addition, support services and information are predominantly communicated in English (or main language used) and therefore may be inaccessible (Woodlock et al., 2020). Victims in rural locations or with sexual minority identities (Whitton et al., 2019) are at increased risk of experiencing TFIPV, as well as sexual exploitation and IBSA (e.g., making threats to humiliate) (Harris & Woodlock, 2019; Woodlock et al., 2020). For victims from sexual minority backgrounds, part of the TFIPV experienced included perpetrators leveraging anti-sexual minority stigma against victims and outing (e.g., stereotypes about certain sexual minorities who are attracted to more than one gender- such as promiscuity- used against the victim online; Leitao 2019b; Whitton et al., 2019). Being in a same-sex relationship was also cited as a vulnerability factor for experiencing TFIPV for those with enough sexual minority participants in their samples to discern this (Borrajo et al., 2015a). Whitton et al. (2019) also found that for sexual and gender minority youth, experiencing TFIPV victimisation was more likely than perpetration.

Another vulnerability factor is that victims who share children with a perpetrator may not be able to disengage from digital communication channels due to parenting arrangements. Perpetrators who use child contact as an avenue to continue harassment and intimidation can also leverage the technologies used by children (devices and SNS) to monitor and harass

their adult victims (Levy & Schneier, 2020; Tanczer, Lopez-Neira, Parkin, Patel & Danezis, 2018; Woodlock et al., 2020).

Victims are at risk of re-victimisation/secondary victimisation from accessing services and support due to lack of standardised protocols of responding to TFIPV, such as lack of communication between family services and IPV services, failing to recognise technology use as abusive in family mediation, or attributing excessive communications as mere annoyance rather than a risk factor for escalation of violence (Woodlock et al., 2020). Victims may also be pressured by first responder services (e.g., the police) to switch off their online presence or phones and replace devices; aside from being impractical, expensive and placing the onus for safeguarding on the victim, this advice may also put them at greater risk as perpetrators will know that the victim is trying to create distance and thus may retaliate via other means or in person (Freed et al., 2019; Leitao, 2018; Maple, Short & Brown, 2011; Worsley, Wheatcroft, Short & Corcoran, 2017). Finally, the burden of avoiding or responding to TFIPV is overwhelmingly placed on the victim, primarily by restricting or managing their online presence. This can result in further victim-blaming and being unfairly judged for the actions they do or do not take, or if they are viewed as not complying with a recommended course of action (Melander, 2010). Harris and Woodlock (2019) reported how victims of TFIPV had been made aware by law enforcement officers that they were expected to cease using technology to combat TFIPV; furthermore, some victims noted that these officers tended to blame them for volunteering information online and appearing reluctant to change their online habits.

The suggestion to move entirely offline is also problematic as victims use online communication as a form of support. Leitao (2019a) analysed over 700 posts in victim support online forums and found that victims use these online communities to share experiences and advice on how to best tackle TFIPV. Victims use technology for social support (e.g., communication with friends and family on SNS) as well as to gather evidence to prove their experiences of TFIPV. TFIPV survivors also exchange advice on digital privacy and security (e.g., covering digital footprints, dealing with hacked/hijacked accounts and spyware, how to block or manage communications with perpetrators). This study further supports the argument that advising victims to go offline may pose additional risks for victims' safety and mental health, as they would lose a significant source of support and information.

Technological Vulnerabilities

Researchers have recognised that there are specific technological vulnerabilities for victims that exacerbate the risk of TFIPV. Technology is evolving rapidly, therefore the average user may take time to become familiarised with the different types and uses of various devices and may therefore be less knowledgeable about privacy and security issues and how to manage their device settings (Leitao, 2019b; Perry, 2012). Professionals—such as social workers, case managers and legal representatives—who work with victims also do not necessarily have the complex cybersecurity knowledge needed to effectively provide aid (Freed et al., 2019). The main technological vulnerabilities identified in the research literature are having weak, known or easily guessed passwords; using Android phones (as opposed to iOS phones) where applications can be installed and run in the background without the victim’s knowledge (Harkin & Molnar, 2020; Parsons et al., 2019); and using shared Smart home devices (IoT; Leitao, 2018).

Sharing a physical space with an intimate partner is common, but this proximity offers perpetrators physical access to victims' devices, whereupon information can be monitored via shared devices such as laptops, desktops, common backup systems or IoT. Unlike a digital privacy threat conducted remotely, shared physical spaces may pose additional vulnerabilities for victims such as physical, sexual and financial abuse. Perpetrators may have access to private information such as medical, lawyer or therapist communications that they could use as part of an intimate attack (Leitao, 2019b; Levy & Schneier, 2020).

IoT devices and systems are often difficult for victims to recognise as forming part of TFIPV. They are newly understood as being employed as part of TFIPV, so no clear guidelines exist to help victims recognise patterns of abuse (Alshehri et al., 2020; Leitao, 2019b; Tanczer et al., 2018). Victims of TFIPV perpetrated via IoT are at risk of not being adequately supported and advised due to the lack of awareness and capacity of statutory and voluntary organisations to deal with these types of technology (Alshehri et al., 2020; Freed et al., 2019; Tanczer et al., 2018).

What evidence exists about the scope/prevalence of different types of TFIPV experienced by adults?

The assessment of TFIPV research indicated a range of variable results which rendered the assessment of the scope and prevalence of TFIPV among adults difficult. Several reasons for this exist. First, some studies did not report prevalence rates in their findings. Of those which did, these rates varied considerably. Some systematic reviews of TFIPV have indicated a range in prevalence rates from less than 1% through to approximately 78% depending on what was being measured, and how (Fernet et al., 2019). Second, the age range of the sample populations varied considerably, with researchers including participants in a variety of age brackets from 11 years upwards. In addition, there was no clear indication or consensus around the age at which researchers demarcated adulthood in studies within or across different nations/states.

Third, the studies employed several different measurement tools which assessed and described different types of TFIPV behaviours. Even among research which utilised the same tool, notable variations in application existed. For example, in their systematic review of TFIPV, Caridade, Braga & Borrajo (2019) identified a range in perpetration prevalence rates, from 8.1% among USA youth (Yahner et al., 2015) to 93.7% among Spanish adolescents (Sanchez et al., 2015). This variation was also present when the same measurement tool (CDAQ) was employed across studies, although within a smaller range (between 49.6% and 88.4% for controlling behaviours, and 10.6% to 14.7% for online direct aggression).

Fourth, studies employed variable timeframes within which they counted experiences of or engagement in TFIPV perpetration. The most recent timeframe for experiencing or perpetrating TFIPV was within the previous week while other studies sought to account for the previous 6 months or 12 months. Caridade et al. (2019) indicated the variance of victimisation rates across studies according to when these were measuring experiences;

those within the previous week accounted for lower rates (5.8%) while those within the previous year accounted for higher rates (92%). Therefore, researchers who allowed a timescale of up to the previous 12 months usually found higher prevalence levels among their sample where at least one form of TFIPV had been experienced in a current or former romantic relationship (Burke et al., 2011; Hinduja and Patchin, 2020; Reed et al., 2019). However, other research did not stipulate any timeframe and so included any instances of victimisation or perpetration ever experienced by participants.

Fifth, while most studies required participants to have been in a romantic relationship within a particular timeframe to meet the sample criteria, the behaviours being researched varied in respect of whether they related to current or former partners. This made determining exposure to repeat victimisation difficult. Sixth, the studies used a range of terminology to describe abusive experiences or behaviours which may have resonated differently among participants with regards to their subjective understandings of what constituted abusive behaviour. For example, some ambiguity exists around certain behaviours outlined in surveys (e.g., swearing) which might form part of a person's vocabulary and not necessarily be an indication of, or intention to demonstrate, hostility. As TFIPV is a dynamic (rather than static) form of victimisation (e.g., is unlikely to be limited to a single incident) and the research participants usually of a younger age cohort, some variability in response to perceived harms may have been present.

Finally, larger female than male samples were common in the research, with some studies only including female participants. Some of the studies which included male participants found that they were more likely to indicate experiencing TFIPV victimisation than the female participants (Hinduja & Patchin, 2020; Lara, 2020). Other studies indicated disclosure discrepancies between female participants' experiences of online and offline TFIPV; information about offline experiences was more readily volunteered without prompting whereas online experiences often emerged as a result of direct questioning (Douglas, Harris & Dragiewicz, 2019; Messing et al., 2020). These findings suggests that TFIPV behaviours may be more evident to male participants than female participants due to holding different behavioural expectations, thresholds or tolerances. Qualitative research by Brown, Flood, and Hegarty (2020) demonstrated that female participants referred to gendered stereotypes when discussing TFIPV experiences (e.g., previously held expectations that young men would control and monitor the social media communications of young women in romantic relationships) while male participants who experienced these behaviours may consider them unusual.

While the abovementioned factors make cross-study comparisons difficult, the following section presents as comprehensive a picture as possible regarding the scope and prevalence of different types of TFIPV as indicated in the included papers.

Victimisation Prevalence Rates

As noted above, determining prevalence rates for experiencing TFIPV victimisation was rendered difficult due to the presence of numerous different variables impeding a meaningful cross-comparison. In particular, Brown and Hegarty (2018) note a variation between studies which measure *abuse* versus *aggression,* with aggression prevalence being higher than abuse prevalence. The most cited type of TFIPV experienced was being controlled or monitored, both covertly and overtly, either through being spied on or having to check in with a perpetrator's request for updates and information about a victim's activities and location (Ellyson et al., 2021). Reed et al. (2020) reported between one-fifth (19.6%) and one-third (33.7%) of participants experiencing TFIPV in the form of digital monitoring and control. Similarly, research by López-Cepero et al. (2018) found rates of between 20% and 30% while Wolford-Clevenger et al., (2016) indicated a 40% prevalence rate for experiencing TFIPV. Woodlock et al. (2020) discovered that almost all (98%) of the practitioners in their study had worked with clients with experience of TFIPV. Nearly half (47%) reported seeing excessive texting and threats to distribute intimate images of their clients, and over one-third (37%) reported seeing harassment via SNS.

Research examining repeat experiences of TFIPV indicated high victimisation prevalence rates. Borrajo et al. (2015a) found that 50% of their sample had been victimised in the past 6 months, with repeat victimisation rates averaging 23 times over this period. Over half (52.4%) of the abusive behaviours had been carried out via SMS or messaging applications, slightly fewer (40.92%) using SNS with the minority (7.4%) being via email. Repeat victimisation was also explored by Trujillo et al. (2020) who found that three-quarters (74%) of their sample had experienced at least one type of TFIPV and one-third (32.7%) had experienced up to three types of abuse. Exploring this in relation to timescales, Flach and Deslandes (2017) stated that young people can experience up to 23 different incidents of TFIPV in periods of less than 6 months. Research with professionals also highlighted the importance of acknowledging repeat victimisation.

High rates of cyberstalking as a form of TFIPV victimisation featured in several studies. Approximately one-third (34%) of the female respondents in research by DeKeseredy et al. (2019) reported being targets of technology-facilitated stalking, which was higher than existing estimates of offline stalking (noted by the authors as usually ranging from 13% to 30%). In their longitudinal study, Messing et al. (2020) reported much higher rates of TFIPV in the form of monitoring, online harassment or cyberstalking among female participants, with approximately two-thirds (60 to 63% across two samples) experiencing this type of victimisation over the duration of the project.

Sexual victimisation emerged as the most studied form of TFIPV with adolescent age groups. Considerable numbers of participants reported having been subject to victimisation related to sexting. Drouin et al. (2015) found that almost one-fifth of their sample (20%: 17% male and 21% female) had been coerced into sexting. Similar rates were reported by Reed et al. (2020) who indicated that over one-quarter (27.2%) of their sample had been pressurised to sext. In a prior study solely focusing on adolescent females, Reed et al. (2019) found that 68%

reported being victims of at least one form of cyber sexual harassment. Of these, the most frequently experienced type involved victims receiving unwanted sexual messages and/or photos (53%), followed by receiving unwanted messages about sexual requests (49%), and being pressurised to send sexual photos (36%). This coercive element was also noted by Ross et al. (2019) with 40% of their sample having experienced some type of coercion, often reporting an overlap between sexual and sexting coercion (21% of participants had experienced both). The researchers also found that women were more likely than men to be coerced into sexting. Finally, Machimbarrena et al. (2018) detailed how 30.27% of their sample had experienced cyberbullying, with 5.79% experienced cyberbullying-sexting (Figure 3 offers an overview of prevalence rates for victimisation).

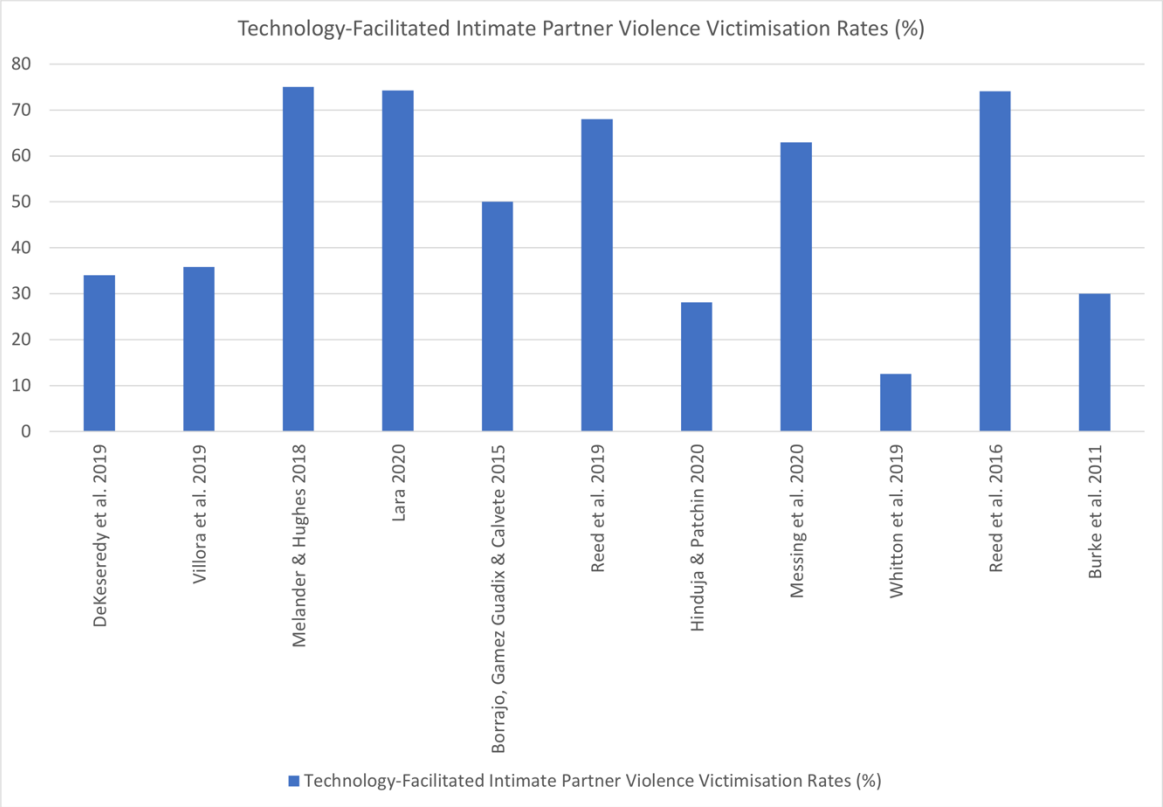


Figure 3: TFIPV Victimisation Rates.

Perpetration Rates

Some studies sought to account for TFIPV perpetration rates among participants. Of these, Levy and Schneier (2020) found that almost one-third (31%) of participants admitted to looking through another person's phone without permission. This was similar to research conducted by Doucette et al. (2018) who found that 37.2% of their adolescent female sample had looked through a partner's cell phone at any time, with 30.8% having done this in the past 3 months. Furthermore, a significant proportion (70.5%) had ever checked up on partner's social networking site, with over half (56.4%) having done this in the past 3 months.

41% indicated that they had had gone through partner's text messages ever, with 29.5% having done this in the past 3 months.

Monitoring and tracking behaviours were also reported by Dardis and Gidycz (2019), who found that almost half (48%) of the women and one-third (34%) of men in their study had engaged in minor cyber unwanted pursuit, with this falling to 11% of women and men engaging severe cyber unwanted pursuit. Similar behaviours were indicated by Watkins et al. (2020) where 57.7% of sample (University students) reported perpetrating TFIPV, cyber stalking intimate partner abuse (67.8%), and cyber sexual intimate partner abuse (10.5%). With regards to controlling behaviours, Gilchrist et al., (2017) found similar rates of perpetration among their participants in England (64%) and Brazil (65%), but more of a difference for perpetrating TFIPV (33% and 20%, respectively). Figure 4 offers an overview of perpetration rates identified in this literature.

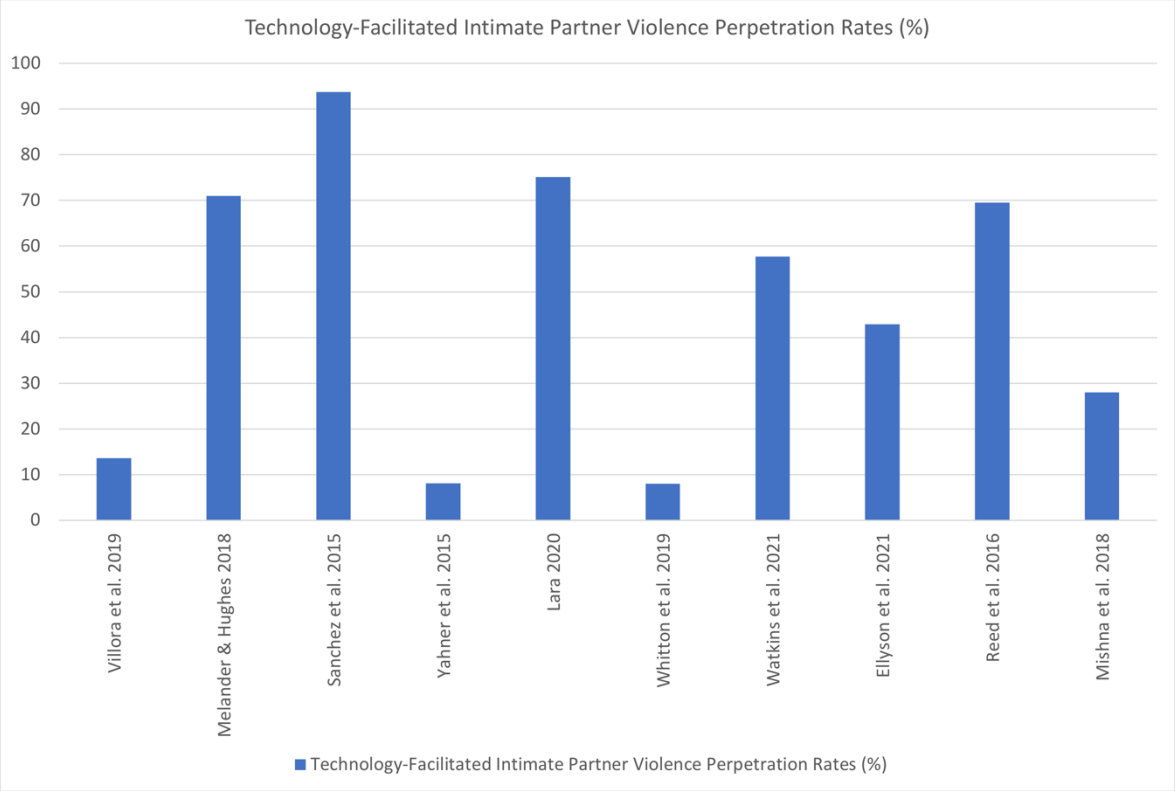


Figure 4: TFIPV Perpetration Rates.

Victimisation and Perpetration Rates

Many studies employed measurement tools which sought to account for both victimisation and perpetration behaviours among the sample. Those which reported a co-occurrence of both in emerging adults and college/university students suggested that mutual TFIPV patterns exist within romantic relationships (e.g., control, partner monitoring via electronic devices and SNS) (Brem et al., 2019; Kellerman et al., 2013; Ross et al., 2019; Villora et al., 2019).

Research investigating co-occurrence in the previous year reported high prevalence rates among participants. Melander and Hughes (2018) found that 71% had perpetrated and 75% had been victimised by at least one TFIPV behaviour, while Reed et al., (2016) found that 62.6% had perpetrated and 68.8% had experienced TFIPV in this period. These rates reduced accordingly when the time period under investigation was shortened. Whitton et al. (2019) assessed TFIPV victimisation and perpetration rates in the previous 6 months, finding that 12.5% had experienced victimisation, while 8% had perpetrated.

When no set time frame was imposed on participants' experiences of TFIPV victimisation or perpetration, higher prevalence rates emerged. Reed et al. (2016) found that almost three-quarters (74.1%) of respondents had been victims of TFIPV at some point during their lives, with 69.5% having perpetrated one or more types of TFIPV. Similarly, Ellyson et al. (2021) noted that over three-quarters (76.1%) of their sample of had ever experienced or used TIPFV.

Exploring TFIPV prevalence and frequency rates, Lara (2020) indicated that three-quarters had been victims and perpetrators (74.3% and 75.1%, respectively) but more notable differences emerged in demarcating frequent victimisation or perpetration (34.3% and 29.5%, respectively). Approximately half reported having experienced (50.3%) or perpetrated (54.8%) the checking of social connections via mobile phone applications. Over a fifth (22%) experienced this frequently as victims, with slightly fewer (18%) reporting frequent perpetration.

Villora et al. (2019) found higher rates of experiencing both TFIPV victimisation and perpetration (35.8%) compared to victimisation only (8%), and perpetration only (13.6%). Ellyson et al. (2021) focused on digital controlling and monitoring behaviours, indicating that 42.9% had used and 58.3% had experienced this (with a further 25% using and 49.2% experiencing direct aggression) (see Figure 5 for a representation). Similar findings were presented by Burke et al. (2011) with 50% of their sample either having initiated or been subject to controlling and monitoring behaviours. One-quarter (25%) of the female participants reported monitoring their partner online (compared to 6% of males) while 30% of female participants experienced some form of unwanted cyber pursuit.

Image Based Sexual Abuse (IBSA) accounted for some of the types of TFIPV behaviours reported in studies. Ellyson et al. (2021) found that 12.4% had used, and 36.4% had experienced some form of digital sexual coercion. Similarly, Mishna et al. (2018) found that while one-quarter (25%) had been a victim of IBSA, only 15% reported having perpetrated it. However, IBSA was the least prevalent behaviour in Lara's (2020) study, accounting for just 2% of victimisation and perpetration.

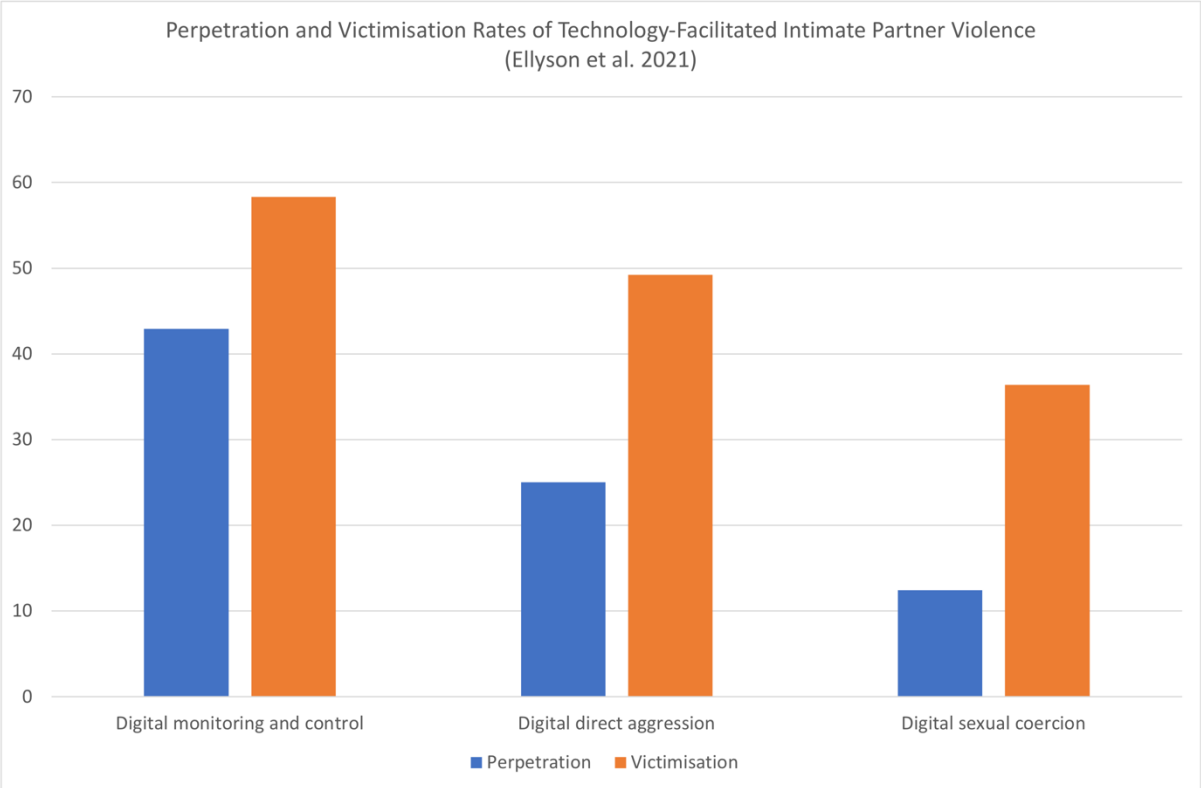


Figure 5: Ellyson et al.'s TFIPV Perpetration and Victimisation Rates.

What evidence exists about the impact of these different types of TFIPV experienced by adults?

The predominance of quantitative studies exploring TFIPV prevalence rates and incident types means less is known about the specific impacts of TFIPV, or how this might compare to offline forms of IPV. No studies in the review sought to explore the impact of engaging in TFIPV for perpetrators.

Understanding the impact of TFIPV on victims is necessary to discern, among other things, the potential ramifications for victims; what type of additional help or assistance victims may need (both at the time and after the incident); and what coping or adaptive strategies victims may employ to manage or cope with TFIPV. A focus on victim impact can also be useful in determining patterns and trends in TFIPV behaviours; this would best be served by a longitudinal study, but very few of these were available for review. The predominant impacts to arise from the review of the literature concentrated on psychological distress; online and social withdrawal; perpetrator omnipresence; and the online/offline nexus.

Psychological Distress

A range of negative psychological and mental health impacts were indicated in many of the studies addressing TFIPV, albeit to such varying degrees and with such variable levels of focus

that cross-comparison was again rendered difficult (Woodlock, 2017; Woodlock et al., 2020; Weathers et al., 2019; Reed et al., 2019; Ellyson et al., 2021; Charak et al, 2019; Hancock et al. 2017; Ross et al., 2019). Of note, however, was that studies which indicated similar TFIPV victimisation (and perpetration) rates among male and female participants discerned a gendered difference in impact, with higher levels of distress among women following TFIPV victimisation than men (Reed et al., 2016; Burke et al., 2011). Victims who had received or been subject to malicious online communications found the re-reading these communications to be re-victimizing in a manner that is unparalleled by offline IPV (Hellevik, 2019).

Victims of TFIPV reported engaging in maladaptive behaviours such as substance misuse (Lu et al., 2018; Melander and Marganski, 2020; Reed et al., 2019; Van Ouytsel et al., 2016) and unprotected sex (Reed et al, 2019; Van Ouytsel et al., 2016), exposing female victims to the risk of STIs and/or unwanted pregnancies. Gracia-Leiva et al. (2020) noted that the bi-directionality of TFIPV did not reflect the predominance of suicidal ideation among women. Female victims of online IPV were at a higher risk of suicidal ideation and suicide attempts, whereas female victims of online *and* offline IPV were at an even higher risk of both suicidal ideation and attempt.

Online and Social Withdrawal

Weathers and Hopson (2015) and Weathers et al. (2019) found that women reported maladaptive coping strategies such as silencing themselves to avoid conflict, constantly monitoring what they discuss in front of their partners, or what their social media profiles contain, to avoid inflammatory content or subjects, going above and beyond to please, and actively avoiding SNS and calls or texts which lead to feelings of stress, anxiety, and isolation, impacting their mental health and wellbeing. The isolation some victims experienced because of TFIPV was compounded by their avoidance of using social or media technologies due to the loss of supportive networks (Clevenger & Gilliam, 2020; Douglas, Harris and Dragiewicz, 2019; Weathers, Canzona and Fisher, 2019; Woodlock et al., 2020).

Experiencing digital coercive control was found to deter some female participants from leaving abusive relationships (Dimond, Fiesler & Bruckman, 2011) or to experience perpetrators blackmailing them in ways that ensured the abuse continued (Vitis, 2020). Victims were particularly afraid of public humiliation via social media and monitoring facilitated by some SNS (e.g., Facebook). Studies cited the growing normalisation of online communications, with this fast becoming the standard means of interaction between young people and emergent adults. This normalisation was indicated as having led to higher thresholds for tolerance of abuse among some young people who were more accepting of some level of monitoring and surveillance from partners (Ellyson et al, 2021). Conversely, this normalisation also had detrimental impacts; young people with prominent levels of social connection felt that this type of abuse was akin to having their 'whole life' taken over, when perpetrators had control over their social media (Hellevik, 2019). Similarly, the psychological harms of online abuse included the victim's anxiety at personal or intimate images shared without their consent being constantly available on the internet (Henry, Flynn & Powell, 2018). Victims therefore felt isolated during or in the aftermath of TFIPV when perpetrators had shared private material with the victim's social circle, or because victims were not

considered as taking the relevant steps to protect themselves from further or future victimisation (Woodlock et al., 2020; Yardley, 2020).

Perpetrator Omnipresence

The omnipresent nature of technology can have a chilling effect on victims who feel unable to separate, distance or protect themselves from a perpetrator, either online or offline as creating distance from TFIPV perpetrators can be more difficult for victims to manage in online environments. Impeding access proved more difficult when perpetrators were cyberstalking or monitoring victims via the social media accounts of shared friends or family members (Burke et al., 2011; Dimond et al., 2011; Woodlock, 2017). Both Woodlock et al. (2020) and Yardley (2020) identified that victims are impacted by the omnipresence of technology (e.g., constant, and relentless intrusions from multiple channels of communication) leading to their harbouring perceptions of not being able to escape the abuse.

The impacts of omnipresence can be far reaching, with victims feeling controlled or isolated in the moments in-between perpetrator activities or actions. Studies cited victims taking measures such as obtaining new mobile phones under different names to avoid being searchable or installing software which blocks unwanted calls or messages to impose a blanket ban on selected callers (Dimond et al., 2011). Dimond et al. (2011) also detailed how the female victims in their study limited their online presence to avoid abuse or contact from the perpetrator. This was especially pertinent given that the women were living in a domestic abuse shelter and feared having their location made known to the perpetrator (e.g., if spyware or tracking applications had been installed on their phones).

Online/Offline Nexus

Studies which explored participants' experiences of both online and offline abuse noted considerable variability concerning the impacts and effects of experiencing both types. Stonard et al. (2017) found that male participants found TFIPV less impactful than offline abuse, while females found it worse as it was considered potentially relentless and unlikely to end with the relationship. Hellevik (2019) noted that some victims had a higher threshold for tolerating online abuse due to the lack of physical proximity to the perpetrator and subsequent perceived lack of immediate physical harm. While some cases of TFIPV involved no direct physical harm caused to the victim by the perpetrator, the unhealthy and unwanted behaviour perpetrated towards the victim was considered akin to aggression nonetheless (Reed et al., 2016).

Considering TFIPV as a form of aggression was important for predicting offline abuse, as several studies indicated that victims of TFIPV later also experienced offline abuse (Duerksen & Woodin, 2019b; Hellevik, 2019; Marganski & Melander, 2015; Taylor & Xia, 2018). In other cases, both online and offline IPV were experienced by victims simultaneously (Hinduja &Patchin, 2020; Doucette et al, 2018). Hinduja and Patchin (2020) explored the connection between online and offline IPV in their sample. They found that 28.1% of the participants who had been in a romantic relationship at some point in the previous year had been the victim of at least one form of TFIPV; while 35.9% had been the victim of at least one form of offline IPV behaviour. Upon examining the relationship between online and offline abuse and violence,

they found that 81% of participants who had been subject to online abuse had also been targeted for offline abuse, while 63% of participants who had been a victim of offline violence also reported experiencing a form of online violence. Research also indicated that victims of TFIPV would attempt to manage this in a similar manner to victims of offline abuse, yet these techniques were often futile as they did little to abate their exposure to TFIPV (Weathers et al., 2019).

What are the gaps in the research related to TFIPV and what are recommendations for future research, policy, and practice?

The difficulties in seeking generalisability or undertaking cross-sectional analysis of the research findings have been outlined above. However, it is worth also noting that efforts to gain a comprehensive picture of TFIPV will be further impeded by the rapidly evolving nature of technology and normalisation of online communicative behaviours. Nevertheless, the following section offers some insight from the reviewed literature into discernible research gaps, along with recommendations for future developments in research, policy and practice.

Gaps in TFIPV Research

Very few studies explored specific vulnerability factors for TFIPV victimisation; those which referred to vulnerability did so in an inconsistent manner, therefore discerning vulnerability factors in a definitive way proved elusive. While it would appear that being younger in age is a potential risk factor for experiencing TFIPV, there was a significant lack of research exploring TFIPV among people aged over 40 years old. Minimal studies included participants aged in their late 20s to mid-30s, but none exclusively sampled an older age group. With increasing numbers of people of all age ranges conducting large parts of their lives online—particularly following the onset of COVID-19— it appears remiss to omit anyone aged over 30 years from studies into TFIPV.

The nature of the relationships within which TFIPV manifests can range from brief encounters through to marriage. Understanding patterns and trends in behaviours necessitates a more representative sample base and engagement in longitudinal research. While some studies explored practitioner experiences, minimal research is available on members of the voluntary and statutory sectors who work with victims and perpetrators of TFIPV, as well as with victims from LGBTQI communities (e.g., Charak et al., 2019; Trujillo et al., 2020).

Much of the available research originates from Northern American countries, with limited studies outlining TFIPV in the following regions: Middle Eastern and North African countries; Sub-Saharan African countries; Southern Asian countries; South-Eastern Asian countries; Eastern European countries; Central European countries; Central American countries; Southern American countries; and many Western European countries, including the UK.

The North American focus also takes a predominantly quantitative approach, often employing and reporting on survey data. There is a significant lack of qualitative investigation into the

context of TFIPV perpetration and victimisation, or the static versus dynamic nature of TFIPV impacts on victims. Similarly, while the participants' gender was recorded as part of the demographical overview, little contextualisation was given to the potential differences informing gendered experiences of TFIPV in many of the studies. Care is needed when interpreting study findings and inferring gender symmetry in cases of TFIPV perpetration. Like offline IPV, context and consequence are crucial aspects shaping victims' experiences of TFIPV, which may range from being considered inconvenient through to intimidating or inducing fear (Brown, Reed & Messing, 2018).

Future Research Recommendations

A key finding to emerge in the review was the high prevalence rates among young people and emergent adults who had experienced TFIPV. This was coupled with findings demonstrating this population's higher tolerance for experiencing abuse that is perpetrated online or via technological means. Many studies cited generational changes and young people's increased use of, and engagement with, social and media technologies which meant that TFIPV was becoming increasingly normalised (Harkin et al., 2020; Lara, 2020; Parsons et al., 2019; Weathers et al., 2019). Victims are more accessible, and the abuse was not limited by time of day or the perpetrator's proximity to the victim.

The growth in ownership of mobile technologies and online accessibility means an increasing normalisation among young people communicating via online mediums or social media platforms. This lack of physical proximity and interpersonal interaction has been suggested as creating a hierarchy among some victims of TFIPV where online victimisation is considered less harmful than offline (in person) abuse. At the same time, it is important to consider online relationships as equally valid and impactful (if not more for some) as offline relationships (Stonard et al., 2017), especially as online communications are increasingly prevalent among younger people and emergent adults. Similarly, studies which indicated that some young people interpreted controlling behaviours as demonstrations of care or love demonstrate the need for healthy relationships education which clearly delineates acceptable and unacceptable conduct (Borrajo et al., 2015b).

It is important to note the impact of terminology use in studies examining TFIPV. The language used in studies should be reflective of the desired population, but this can impact on findings if samples are comprised of different generations with varied interpretations of relationship descriptors. In many of the North American studies, the most popular term used to describe romantic relationships was 'dating'. However, many young people do not use 'dating' to describe their romantic and/or sexual relationships (Rothman et al., 2021). Similarly, older people may be subject to TFIPV in current or former long-term, committed relationships but may not recognise that as 'dating' violence in the same was as someone who is newer to romantic relationships.

The use of measurement scales to provide a snapshot of behaviours among a particular cohort risks missing valuable information through results standardisation; for example, the differential impact of minor versus severe (or singular versus repeated) acts (Wolford-Clevenger et al., 2016). While it is important not to consider frequency an indicator of severity (Lara, 2020), studies are currently unable to indicate whether a victim is more impacted by a single incident of TFIPV or a series of incidents. Similarly, the point at which victims of

repeated TFIPV become desensitised to the abuse is important to discern as this may alter their survey responses. Qualitative research can therefore provide greater insight into the contextual factors informing people's experiences of, and responses to, TFIPV. It is recommended that the findings from qualitative research are used to provide greater insight and understanding.

The predominance of cross-sectional studies in the assessment indicated a trend towards research which captures a snapshot of TFIPV among certain populations. There was a lack of longitudinal studies or qualitative studies, both of which offer important information about the nature and impact of TFIPV, particularly if this is experienced as a repeat or ongoing behaviour. Linked to this, few studies investigated experiences or perpetration of offline abusive behaviours. Of the studies which did, a link was noted between perpetrating offline and online abuse suggesting that these need to be explored together.

While it did not feature as one of the REA questions, it was notable that none of the assessed studies examined the presence or effectiveness of TFIPV prevention strategies, treatment or interventions (with the exception of Hertlein et al., 2020). Future research into TFIPV should include examination of interventions and treatments in traditional and non-traditional couples (LGBTQI and polyamorous) to provide insight (Caridade et al., 2019; Hertlein et al., 2020).

Legislation and Policy Recommendations

As many studies focused on emerging adults, often during their time at college or university, they highlight the prevalence of TFIPV in this population. Some also outlined the responsibilities of higher education institutions to increase awareness on campus, have mandatory education programmes teaching online citizenship and etiquette, bystander intervention and also have trained specialists on campus to identify and report TFIPV (Cantu & Charak, 2020). However, as noted above, the majority of these studies originated in North America, where the legislative framework around student sexual violence is very different to the rest of the world, since educational establishments are subject to Title IX and The Cleary Act, which are nationwide laws governing institutional reporting and policies around campus violence.

Nonetheless, educational investment is important since suggesting that people avoid being online is futile, unhelpful and possibly more harmful due to the potential for exacerbated isolation and impediments to seeking help and advice (Dimond et al., 2011). Campaigns for education around security and risks need to target both young and other adults (Witwer et al., 2020), in accessible language, and in online platforms that are most likely to be used by each age category (e.g., TikTok for adolescents, Facebook and Instagram for emerging and other adults).

Studies indicated the range of reasons impeding victims from seeking help from authorities. These included feeling embarrassed (Woodlock, 2019); being, or feeling, shamed (Vitis, 2020); and experiencing negative responses, especially from the police (i.e., dismissal and/or victim-blaming) (Harris and Woodlock, 2019; Powell and Henry, 2018). These studies recommended better training and education for authorities and criminal justice practitioners (Witwer et al., 2020), along with alerting them to the difficulties victims might encounter when seeking help

(Douglas et al., 2019). Advocating for better policy guidance (Messing et al., 2020) and legislative clarity (Powell and Henry, 2018) is particularly important as TFIPV not only erodes public and private boundaries but may also impact on physical ones.

To respond effectively to victims who report TFIPV, authorities will require evidence of the harms they have experienced (Witwer et al., 2020). Some victims indicated that they used technology to record evidence of the abuse (Douglas et al., 2019). Where victims are unaware of how to do this, or the potential need for it, agencies should be able to assist or advise victims seeking to collect such evidence. Research also indicated high rates of poly-victimisation among victims of TFIPV, prompting suggestions of preventative approaches for victims that acknowledged and addressed the multiple risks victims may encounter (Machimbarrena et al, 2018). The online nature of TFIPV, mediated through mobile and social technologies, means educational interventions may be best facilitated in an online manner.

Public Health Recommendations

Several studies recommended more support for practitioners to recognise and respond to TFIPV, particularly if victims were more likely to engage with them as a result of their experiences (Harris & Woodlock, 2019; Douglas et al., 2019; Powell & Henry, 2018). It is important to note the gender dynamic informing thresholds for tolerance of abuse here; young women may be less likely to disclose abusive behaviours if they have been conditioned to see these as protective rather than abusive.

Cantu and Charak's (2020) study showed that types of TFIPV such as psychological and sexual cyber abuse are uniquely predictive of depression, and that psychological, sexual, and stalking types of TFIPV have a cumulative effect on depression and mental health, thus making it imperative to look at TFIPV as a multidimensional form of interpersonal violence. Furthermore, depression should be probed by clinicians working with emerging young adults in intimate relationships for the presence of TFIPV.

Couples' therapists and clinical practitioners lack training and protocols in recognising and responding to TFIPV (Hertlein et al., 2020; Leitao, 2018). Clinical assessment and evaluation for TFIPV needs to be structured, include a specifically developed assessment tool and include all aspects associated with the behaviour and its risks, including coercive control as this is the method with which it manifests. All practitioners dealing with IPV and TFIPV need to be appropriately trained using specifically tailored training manuals.

Cyber Security Recommendations

Studies highlighted the need for better accountability from social media organisations, app developers and technology companies (Messing et al., 2020; Harkin et al., 2020; Parkin et al., 2019; Parsons et al., 2019) coupled with addressing obstructive behaviours from social media organisations (Powell & Henry, 2018). App and technology developers should create interfaces and devices with easy to manage privacy and security settings, written in accessible language for the average user, and consistency across devices/interfaces in IoT setups (Leitao, 2019b; Parkin et al., 2019).

Codesign methodology has been adopted by researchers (e.g., where users or stakeholders are included in the research and give recommendations; Leitao, 2018; 2019a; 2019b); through

this method, victims have given several recommendations based on their experiences such as multi factor authentication and biometrics to be added to device and account management (so that perpetrators' access to them is hindered) and visual or auditory signals when devices are recording or are activated.

Cybersecurity academics, practitioners and independent charities have recognised and recommended that victims of TFIPV need specific technological advice and help after a TFIPV attack, to secure their devices and networks and remove specific content or applications. Several have made efforts to systematise the various digital attacks seen in TFIPV, identify the complexity of advice and intervention needed by victims, as well as set up protocols for responding, and engage in clinical computer security services that offer online and in person consultations to victims of TFIPV (e.g., Freed et al., 2019; Havron et al., 2019). The majority recommend a client-centred approach and start from referrals by IPV professionals; the protocols include a 3-pronged approach of a) *understanding* the client's digital footprint and complexities, b) *investigate* their devices, services and apps to assess problems and c) *advise* clients how to proceed. Questionnaires or interviews are used to assess technology issues of clients, a summary of clients' digital assets (technograph) is produced and specifically formulated tools for detection of malware, applications and system compromises are developed and used (e.g., Havron et al., 2019)

It is recommended that clinical security services should be widely accessible and recognised as part of TFIPV response. Victims have complex and unique needs, and they often do not come to consultations with a clear view of what these needs and priorities are. Practitioners offering technological assistance to TFIPV victims need to help victims identify their vulnerabilities and safeguarding issues of pressing importance as well as work with different support organisations and IPV professionals to determine risk of physical as well as technological abuse. IPV professionals and clinical computer security specialists will need to share knowledge regarding risk and advice on how to document and respond to TFIPV. Furthermore, clinical techniques and security services will need to be adapted to specific geographic locations and take into consideration the variability in legislation (Havron et al., 2019; Lopez-Neira et al., 2019).

Discussion

We undertook a thorough review of the literature using a Weight of Evidence (WOE) approach, frequently adopted in Rapid Evidence Assessments (e.g., Davidson et al., 2019; EFSA, 2017; Horvath et al., 2013). We examined over 4500 sources, identifying nearly 200 peer reviewed papers and policy reports that were relevant to TFIPV, and selected 103 sources that were deemed to have either high or medium trustworthiness in answering the 6 questions pertaining to TFIPV that were set out in this assessment (e.g., typology, perpetrator characteristics, victim vulnerabilities, prevalence, impact and gaps). Most of that research focused on North America, with some studies addressing Australia, Canada, Spain, Singapore, Peru and the UK. There was a low representation of non-Western diaspora populations.

The main difficulty encountered during searches for this REA and with the synthesis of available evidence was the lack of definitional synergy and terminology used to describe

TFIPV. Varying terms and definitions may not adequately capture all implicated behaviours and will not be recognised at all times by participants of varying demographic characteristics. This disparity causes significant difficulties in interpreting research results as well as estimating accurate prevalence rates for TFIPV (prevalence rates varied considerably from 1-98% depending on behaviour measured and methodology).

Available data from IPV services (e.g., police, helplines and shelters) revealed that during the COVID-19 pandemic there was a 70% increase in victim contact with these services, and that the majority of women who came into contact with Refuge (one of the largest DVA/IPV charities) had at least one experience of TFIPV. In the last 3 years there has been a sharp increase in attempted and completed commercial spyware application installations (nearly 400%; The Kaspersky Security Network), denoting a significant prevalence, shift in new methods used in TFIPV perpetration as well as the normalisation and commercialisation of abusive behaviours (e.g., monitoring, accessing information without consent).

Social media remains one of the most frequently used technological methods of perpetrating TFIPV (particularly Facebook) and social media and mobile technology use is simultaneously a predictor for perpetration (Duerksen & Woodin, 2019b) but also victimisation (e.g., more possibilities for exposure; Melander & Hughes, 2018). Several sources highlighted that the way SNS are set up, creates a conducive and normalising environment for monitoring, controlling and inflammatory behaviours online.

TFIPV behaviours can be summarised in 4 broad types: Cyberstalking and coercive control, Harassment, Image Based Sexual Abuse and Indirect non-sexual abuse, with monitoring and control and harassment (via social media and email/text/instant messaging) being the most prevalent types. It was consistently indicated in the literature reviewed that TFIPV was correlated and linked to offline IPV perpetration, and that mutual patterns of abuse exist in romantic relationships where perpetration and victimisation are experienced in tandem.

We were not able to establish clear gender patterns from the data and studies reviewed, and gender does not appear to be a significant predictor for either perpetration, or victimisation of TFIPV. Some interesting differences in motivation and type of TFIPV behaviours were noted by some researchers (e.g., Brown et al., 2020; Dardis & Gidycz, 2019; Pineda et al., 2021; Smoker & March, 2017), such as females perpetrating more covert and less serious forms of TFIPV (e.g., monitoring a partner's access and use of SNS or phones) compared to males' more overt and severe TFIPV (e.g., antisocial, predatory, IBSA behaviours).

Perpetrator profiles were also difficult to establish from the literature, but some predictors of perpetration were confirmed such as negative affect, jealousy, dark personality traits (e.g., Machiavellianism, narcissism, psychopathy and sadism), attachment anxiety, substance and alcohol abuse, and SNS use. An interesting finding was that perpetrators most often will use and abuse their knowledge of victims and their ownership-based access (e.g., exploiting their legal ownership of victim's devices, or shared home devices), or will attempt to compromise victims' accounts and devices (e.g., guessing passwords, hacking, installing spyware) to exert control.

Offline IPV was recognised as the highest victim vulnerability and risk for TFIPV. Disabled, linguistically diverse, learning disabled and sexual minority individuals are at higher risk of TFIPV and may have difficulty accessing support. Women overall report greater impact as well

as risk of TFIPV than men and victims who share children with perpetrators of TFIPV report additional impacts to the level of harassment and intimidation as well as increased difficulty to escape the abuse. The severe psychological and mental impact of TFIPV on its victims has been clearly demarcated in the literature (e.g., stress, isolation, anxiety, self-harming and even suicide). Due to the online nature of the abuse, where perpetrators can contact and abuse victims in various ways with minimal effort and without the need of physical proximity, victims often report the perpetrator omnipresence and inescapability of the abuse.

A significant converging point for almost all papers reviewed, was that the nature of fast evolving technology is making examining and tackling TFIPV challenging. Professionals responding to TFIPV often lack the sophisticated technical expertise necessary to help and advise victims on security. Moving forward, and to keep up with rapid developments in technology, stakeholders highlight the pressing need for social networking platforms and tech companies/developers to take responsibility for their interfaces and how these proliferate TFIPV and facilitate perpetration, as well as assume their duty of care towards all users. Researchers from multiple disciplines also call for a synergistic relationship between the voluntary and statutory sector professionals who encounter victims of TFDA. Clear guidelines that can highlight risk and appropriate steps for the immediate and long-term response to TFIPV need to be developed in consultation with frontline practitioners (e.g., cybersecurity specialists, police, therapists and other first responder professionals) so that we can identify and sanction perpetrators and better support victims of TFIPV.

Workstream 2: An analysis of a representative sample of TFIPV cases reported to The Cyber Helpline

Workstream Description

Workstream 2 was developed, led and completed by PI Dr Jennifer Storey with the help of three PhD level RAs who completed case coding and data consolidation and in consultation with The Cyber Helpline.

This Workstream involved a thorough analysis of the presence of TFIPV in the 4,632 cases of online harm reported to The Cyber Helpline between December 2018 and March 2021. The aim was to identify the prevalence and type of TFIPV perpetrated and the methods of abuse used by perpetrators to commit TFIPV against current or former intimate partners. A secondary aim was to determine whether these variables differed pre- and post-COVID-19 restrictions. For the purposes of this and subsequent workstreams, pre-COVID refers to dates prior to March 23, 2020, and post-COVID refers to March 23, 2020 forward when restrictions were put in place in the UK related to the COVID-19 pandemic.

Introduction

Technology use has become an integral part of our personal and working lives. This has increased as a result of the lockdown measures put in place to manage the COVID-19 pandemic. This shift to online behaviour is also evidenced in the perpetration of IPV, resulting in TFIPV (Christie & Wright, 2020). To best understand and combat this issue, and in addition to the REA in Workstream 1, we must identify its prevalence, nature and the methods by which this abuse is being perpetrated.

The REA identified that the current literature is limited with respect to these areas in several ways. Prevalence rates of TFIPV vary greatly across studies. Of those studies available, few include a representative national dataset and there is a dearth of research from the UK. To date studies have focused on adolescents and young adults with limited work on the adult population. There is also minimal research from voluntary sectors who work with victims of TFIPV. Further, few studies have been representative of different relationship types (i.e., from brief encounters to long-term relationships). In the examination of types and methods most studies have imposed a structure on responses from victims by presuming types and methods of TFIPV in psychometric measurements. This has potentially limited what is reported by researchers and subsequently limited the help that can be suggested and provided to victims.

The present study addresses these limitations by examining a nationally representative sample of cases including individuals of all ages who sought help from a UK not for profit organisation. Relationship type was recorded across all cases and used to examine the potential differences across TFIPV type and the methods employed to perpetrate TFIPV. Further, the sample examined was applied in nature, consisting of reported cases to a UK not for profit; this means that no structure was imposed on the reporting of TFIPV type or method

of perpetration. The information gathered consisted of what victims and concerned persons thought to be more relevant and helpful in responding to their case.

Research Aims

This workstream examined:

(1) The prevalence of TFIPV among cases of online harm reported to a national UK helpline between December 2018 and March 2021.
(2) The prevalence and types of TFIPV perpetrated,
    a. Whether the prevalence and types of TFIPV differed pre and post-COVID-19 restrictions,
(3) The prevalence and type of methods used by perpetrators to commit TFIPV,
    a. Whether the prevalence and type of methods used differed pre and post-COVID-19 restrictions

Method

Overview

Information on the prevalence, type of TFIPV and methods used to perpetrate TFIPV was gathered from 555 reports of TFIPV reported to The Cyber Helpline, a national UK helpline for victims of online harm. Information from cases reported to the helpline via referral, email or Chatbot was recorded electronically by the Helpline Responders. Client records included all contact between the helpline and the client, as well as online forms completed by the client and any notes included in referrals to the helpline. These records included the type of abuse perpetrated and the methods used to perpetrate the abuse, all of which facilitated the helpline's ability to guide and assist clients. Access to records was provided by The Cyber Helpline and the research received ethical approval. Client records were coded by trained research assistants (RAs) using a coding sheet and were anonymized during this process and prior to analysis. The coding sheet was developed based on researcher knowledge of the online harm literature, the expertise of The Cyber Helpline and the review of the helpline database and sample cases. All cases identified as IPV were coded by one of the RAs and then reviewed by a second RA.

Cases

The Cyber Helpline assists victims in the UK at no cost and those outside of the UK at a cost for service. They respond to requests for assistance from victims and concerned persons who typically contact the charity via a Chatbot. The Chatbot attempts to initially classify cases and provide help and cyber-attack guides to victims and concerned persons. Assistance is also provided via referrals and email. If cases are not resolved using the Chatbot, they are passed to a Helpline Responder who communicates with the client to resolve their case. All communication is linked to form a client record.

6,060 client records between 17/12/18 and 23/03/21 were examined for inclusion in this project. First, duplicate cases were also removed from the sample (n = 1428). This left a total sample of 4,632 cases to code. Given our focus, cases of TFIPV were identified and coded in

greater detail. To be included as a case of TFIPV two criteria had to be met: First, an intimate relationship had to be present between the perpetrator and the victim. To be classified as intimate there had to be a relationship in which the victim had engaged with the perpetrator with romantic intent. This included anything from a brief romantic or sexual encounter (online or offline), to dating, to a long-term partnership like marriage. Cases were therefore excluded from detailed coding if other types of relationships (e.g., familial, neighbours) were present or if the perpetrator was romantically pursuing the victim but the victim had never returned that interest or engaged with the perpetrator (4,060). Second, online abuse had to be present in the cases. 17 cases were excluded from detailed coding as there was no online abuse reported between the intimately involved victim and perpetrator. A total of 555 (12%) cases met the inclusion criteria for TFIPV, 4,077 (88%) cases were identified as non-TFIPV. For the purpose of clarity, the targets of TFIPV in those records will be referred to as *victims* of TFIPV, the individual(s) engaging in the TFIPV will be referred to as *perpetrators* of TFIPV and the overarching incident reported will be referred to as the *case*.

Information from client records was coded by three RAs who were PhD level graduate students in Forensic Psychology. Client records contained some demographic information as requested by the helpline such as whether the victim is 18 or older and if they live in the UK. Cases of stalking also included a 'cyberstalking form' with more detailed questions about the stalking behaviour. The type of attack was recorded by the helpline. Although some information was recorded as required in client records (such as attack type), most of the information of interest was not and was therefore coded by RAs from the free-text fields, emails and online-forms contained in the client records using a coding sheet.

Materials

The information available for the present study was that collected in the context of a report of online harm to The Cyber Helpline. No additional scales or questions were added for data collection. Examining the information available to Helpline Responders is critical to understanding the type of information that is reported and what details about the harm can be identified and assessed from the client records.

Client records were coded using a coding sheet to extract demographic information, information on type of attack and method of attack. Demographic information was coded where possible from identified fields in the client records (e.g., age above or below 18) and otherwise from free text (e.g., gender of the perpetrator and victim). Type of attack was coded as it appeared in client records. In each case, the CEO of the helpline identified the type of attack being perpetrated in the case. In some cases, multiple attack types were listed in the client records; therefore, clarification was sought from the Helpline Manager to identify the overarching single attack type for these cases. A list of 40 attack types was developed by the Helpline and updated regularly with new attack types for the purpose of classification. The method by which TFIPV was perpetrated was coded based on free text, and all methods mentioned in client records were recorded on the coding sheet.

The coding tool was developed based on knowledge of the research literature on online harm, IPV and case file review methodologies. It was designed so that no identifiable information was coded or removed from helpline records. After development, The Cyber Helpline cases were reviewed to refine wording of the coding sheet and categories. In particular, the cases

were used to identify attack methods. The coding tool was then reviewed by the multidisciplinary research team and The Cyber Helpline and updates were made.

The coding tool was then trialled by the PI and the RAs on five cases to assess clarity and reliability. Changes were made to clarify definitions. This was repeated twice with RAs coding 15 cases each time and then meeting with the PI to review ratings. This significantly improved the reliability between the RAs and expanded the definitions and methods of attack categories. Finally, 100 cases were coded with the aim of expanding the methods of attack and finalising the coding sheet. The cases were reviewed with the research team and The Cyber helpline to define and classify the methods of attack identified. This procedure greatly increased the number of methods identified and allowed coding of the remaining cases to proceed without having to significantly alter the coding sheet.

Coding decisions were made to increase the quality and reliability of the data collected. First, RAs recorded the attack type decisions of the CEO and did not impose their judgement. This decision was made to reflect the expertise of the helpline. Second, information reported by victims was taken as accurate. For instance, if the victim said that they had been Catfished by a male, then the perpetrator was coded as male. Although we recognise that victims may have been mistaken due to the online nature of the relationships, all files were based on victim reporting and thus necessitated coding of information as reported, as is the case in other types of file review studies.

Procedure

Permission to conduct the study was sought and obtained from the University of Kent Psychology Ethics Committee. The three PhD level Forensic Psychology RAs coded the data. All RAs passed a Disclosure and Barring Service (DBS) check prior to accessing any client records.

RAs underwent extensive training on the data from The Cyber Helpline and the coding procedures from the PI. RAs completed The Cyber Helpline online training course, which includes approximately 6.5 hours of pre-recorded presentations outlining the different cyber issues the Helpline responds to. RAs also participated in live-online training from helpline staff on navigating the case management system. As above, RAs were trained in the use of the coding tool and practiced and refined those skills through the coding of cases. Although this training greatly increased the reliability of the raters, the cases proved to be very diverse in nature and the novelty of the online methods of abuse utilised meant that cases raised many questions. This slowed and broke-up the coding process. Thus, to improve reliability and speed, it was decided that each case would be coded by one RA and reviewed by a second. Any discrepancies were discussed and resolved with the oversight of the PI (with whom no identifying information was discussed) and where needed the assistance of The Cyber Helpline, particularly in relation to clarification of online methods of abuse and for cases which required the addition, or clarification of, attack type. Thus, all cases analysed in this study are the product of consensus between extensively trained PhD level raters.

Cases starting on December 17, 2018 and up to March 23, 2021 were coded. The start date reflects the implementation of a Chabot by The Cyber Helpline to help classify and respond to cases. The end date was selected to reflect one year after the start of the UK lockdown

related to the COVID-19 pandemic. A total of 4,632 cases were coded for inclusion in the study. Given that the charity is national, and the sample is continuous the data is nationally representative of TFIPV victims and concerned persons in the UK who have reached out for formal support.

Data analyses

Analyses were conducted using SPSS v. 26. Descriptive statistics including frequency analysis were used to report demographic characteristics, attack type and method of attack. Chi Square (or Fisher's exact test where cell count was less than 5) and T-tests were used to examine whether differences existed pre and post COVID-19. Missing data is reported for sample characteristics. There were no missing attack types or TFIPV methods so no adjustments were required for inferential analyses.

RESULTS

TFIPV Prevalence and Sample Characteristics

What is the Prevalence of TFIPV among Cases of Online Harm reported to The Cyber Helpline?

A total of 4,632 unique cases were reported to The Cyber Helpline during the approximately 27.5-month period examined. Of those cases 4,077 (88%) did not meet inclusion criteria for TFIPV. A total of 555 (12%) cases could be classified as TFIPV meaning that there was a romantic relationship between the victim and perpetrator and technology facilitated abuse occurring.

Case frequency over time is presented by case type (TFIPV or non-TFIPV) in Figure 6. Non-TFIPV cases were consistently more prevalent over time. An increase can be seen in cases over time as would be expected with increased public awareness of the Helpline. In addition, several spikes in case numbers are also notable. Several reasons are posited for those spikes related to events that increase knowledge of the charity, technical errors in the case reporting system, seasonal changes and the impact of the COVID-19 lockdown.

In January 2020, The Cyber Helpline was featured on ITV; this led to visibility that is reflected in a sharp rise in cases on the graph. Further, in January 2021 The Cyber Helpline conducted training on three occasions for police and charities. These organisations are referral sources for the Helpline and thus may have resulted in more cases due to increased referrals. On several occasions, a technical error caused a delay in cases being uploaded and dated on the Helpline's system, this resulted in large numbers of cases being recorded on a single date. These technical errors are reflected by sharp increases in cases in December 2018 and July 2020. January spikes may also reflect what The Cyber Helpline has generally noticed to be a seasonal increase in cases that occurs after the December holidays. Increased tension and/or abuse during the holidays may lead to a decision by victims to change course in the new year and report problems to authorities.

Even with consideration of all of these impacts on case numbers, a clear increase in cases can be seen just after the start of the pandemic and subsequent lockdown. Pre-COVID a total of 666 cases, 89 (13.4%) of which were TFIPV, were reported, compared to post-COVID where 3,815 cases, 463 (12%) of which were TFIPV, were reported. This equates to a 472.8% increase in cases reported to the Helpline, and a 420.2% increase in TFIPV cases. This suggests that the period of COVID-19 restrictions resulted in significantly more perpetration of online harm generally and TFIPV. Proportionally, as compared to each other, online harm and TFIPV remained the same, with about 12% of cases constituting TFIPV across time.

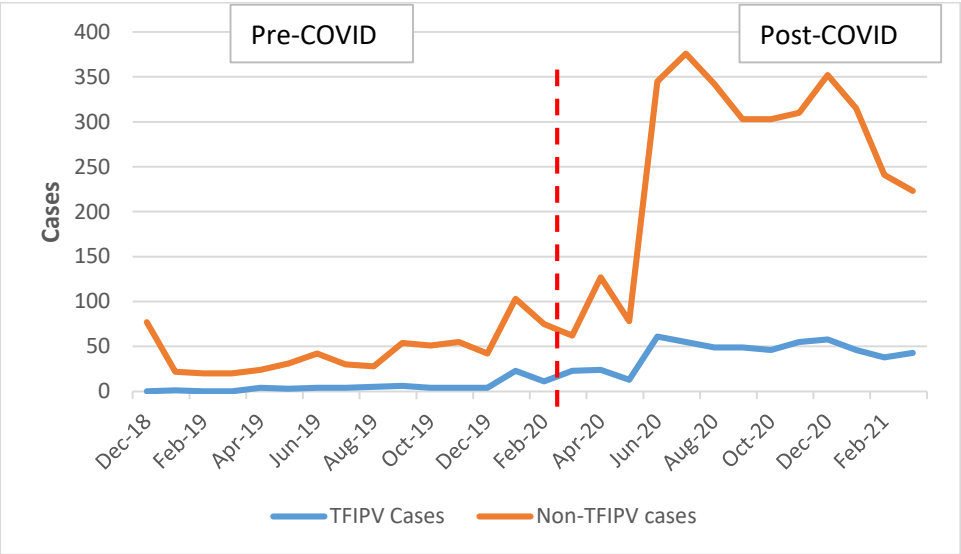


Figure 6: Frequency of helpline contact over time by presence of TFIPV (N = 4,632).

The 555 cases of TFIPV examined between December, 17, 2018 and March 23, 2021 form the basis for all of the analyses presented from here forward. Where comparisons are made related to the COVID-19 restrictions the total number of cases is 552 which occurred between March 22, 2019 and March 23, 2021.

Sample Characteristics

Characteristics of the sample were collected and are displayed in Table 4, for some characteristics there was a substantial amount of missing information. This is to be expected given the applied nature of the sample and the online nature of The Cyber Helpline's work. Studies utilising applied samples often encounter missing data because data are not collected for research purposes, in this case, data were collected for the purpose of assisting victims. Further, the online nature of The Cyber Helpline's work meant that data availability was reliant on victims and concerned persons responding to questions. Helpline workers could not probe for additional information or visually code variables like gender. Nevertheless, where high rates of missing data exist, the sample characteristics reported should be considered with caution.

As reported in Table 4, victims of TFIPV were more often female and perpetrators more often male. Victims were mostly over the age of 18. Victims reporting to the Helpline were most often UK-based, it should be noted that the Helpline's services are only free to those in the UK. Perpetrator location was unclear due to missing information but seemed to be more evenly split between the UK and outside of the UK, which if representative, has implications for legal intervention. Cases were most often reported to the Helpline by the victim, rather than a concerned person.

The most common relationship held between the victim and perpetrator was a brief relationship which could have constituted anything from a one-night intimate encounter to short term dating. Ex-partners, defined as those in longer term relationships were only slightly less common in the sample. Less common relationship types were current relationships, divorced, separated and married, all occurring in less than 10% of the cases. The relationship between the perpetrator and victims in the sample were most often online only, however, just over a quarter included face-to-face contact; cohabitation was rare. In line with this, most attacks were perpetrated entirely online, with 17.5% of attacks also including an offline component.

Information on reporting to police and receiving help from other resources was often missing but suggest that at least 22% of cases were reported to police and a quarter involved assistance from other sources. Victims were asked to indicate whether they felt that they were in imminent danger, most did not respond and a small minority (2.5%) replied that they did. Victims were also asked if they had been threatened with online harm. Again, most failed to respond, but responses showed that over a third had been threatened.

Table 4. Frequency of Sample Characteristics.

Sample characteristics	***n***	***%***
Victim gender		
Female	215	38.7%
Male	69	12.4%
Transgender	1	0.2%
Missing	270	48.6%
Perpetrator gender		
Female	143	25.8%
Male	325	58.6%
Transgender	1	0.2%
Missing	86	15.5%

Victim age		
Over 18 years	237	42.7%
Under 18 years	23	4.1%
Missing	295	53.2%
Victim location		
In the UK	175	31.5%
Outside of the UK	85	15.3%
Missing	295	53.2%
Perpetrator location		
In the UK	101	18.2%
Outside of the UK	63	11.4%
Missing	391	70.4%
Case reported by		
Victim	457	82.3%
Other reporter	98	17.7%
Current relationship type		
Brief relationship	229	41.3%
Ex-partners	219	39.5%
Ongoing relationship	44	7.9%
Divorced	34	6.1%
Separated	18	3.2%
Married	11	2%
Face-to-face or online relationship		
Face-to-face	158	28.5%
Online only	251	45.2%
Missing	146	26.3%

Victim-perpetrator cohabitation		
Yes	4	0.7%
No	415	74.8%
Missing	136	24.5%
Online or offline attack		
Online only	338	60.9%
Offline attack too	97	17.5%
Missing	120	21.6%
Case reported to the Police		
Yes	122	22%
No	63	11.4%
Missing	370	66.7%
Other help involved		
No	7	1.3%
Yes, other charity	47	8.5%
Yes, police	18	3.2%
Yes, other legal	7	1.3%
Yes, physical or mental healthcare	5	0.9%
Yes, council	1	0.2%
Yes, multiple types	65	11.7%
Missing	405	73%
Victim reported feeling in immediate danger		
Yes		
No	14	2.5%
Missing	63	11.4%
	478	86.1%
Threats of online harm		

Yes	203	36.6%
No	1	0.2%
Missing	351	63.2%

Note. *N* = 555.

TFIPV Type

What is the Prevalence and Type of TFIPV Perpetrated?

There were 22 types of TFIPV perpetrated across the 555 cases. One type of TFIPV was identified by The Cyber Helpline per case. TFIPV types, definitions and prevalence are reported in Table 5. To facilitate analysis types were grouped into 5 categories reflecting a common underlying perpetrator behaviour.

Attack category 1 involved *Unwanted contact and communication* by the perpetrator toward the victim. Seven attack types were included in this category and collectively this category was the most commonly perpetrated, occurring in approximately half of cases. Most frequently, *cyberstalking* was the attack type perpetrated to engage in *Unwanted contact and communication*. Attack category 2, *Extortion,* included three attack types characterised by perpetrators who demanded money or favours from victims for whom they possessed compromising information. This category was the second most common, impacting over a third of victims. The use of webcams to take unauthorised images which were then used for blackmail or sextortion was the most common form of this attack. Attack category 3 is *Unauthorised access* which includes nine attack types where the perpetrator gained or tried to gain access to a victim's information, account or device without the victim's permission: most commonly this was done through a social media account. This category was much less common than categories one and two. Attack category 4 involves *Physical device problems* caused by the perpetrator and includes two relatively uncommon attack types: most often issues were related to malware but *IT issues* also occurred. The final attack category 5 is *Theft* which included two uncommon attack types related to perpetrators taking or withholding something that belonged to the victim.

Attack types were examined to determine if variation existed by relationship type. Brief relationships, lasting a few months or less (n = 229, 41.3%), were compared to longer term partnerships (n = 282, 50.8%). Current relationships were excluded as relationship length was not recorded. *Extortion* was more common in brief relationships, $\chi 2(1, N = 511) = 241$, $p < .001$, Phi = .687. *Unwanted contact and communication* and *Unauthorised access* were more common in long term partnerships, $\chi 2(1, N = 511) = 118$, $p < .001$, Phi = -.480, $\chi 2(1, N = 511) = 34.3$, $p < .001$, Phi = -.259, respectively. A comparison using current and past relationships could not be conducted due to the rarity of current relationships (7.9%) in the sample.

Table 5. TFIPV Attack Type Description, Frequency and Comparison Pre and Post COVID-19.

Type of TFIPV	***n* (%)**			***Test of significance* *(t-test, χ, Fishers)***
	Total	**Pre-COVID**	**Post-COVID**	
Unwanted contact and communication	**277 (49.9%)**	**48 (53.9%)**	**229 (49.5%)**	***t*(550) = .772, *p* = .441**
Cyberstalking: *Persistent and repetitive patterns of online behaviour causing the victim fear of violence or alarm and distress.*	143 (25.8%)	34 (38.2%)	109 (23.5%)	$\chi 2(1, N = 552) = 8.36$, $p = .004$, Phi = -.123
Catfishing: *Fake online profiles are used to trick the victim into a romance. The victim may then share private information or send money.*	59 (10.6%)	6 (6.7%)	53 (11.4%)	$\chi 2(1, N = 552) = 1.73$, $p = .188$
Harassment: *Unwanted online behaviour that causes the victim alarm or distress. May cause the victim to feel offended, intimidated or humiliated.*	47 (8.5%)	5 (5.6%)	42 (9.1%)	$\chi 2(1, N = 552) = 1.14$, $p = .285$
Fake profiles: *Fake social media profiles are used to harass or impersonate the victim.*	13 (2.3%)	2 (2.2%)	11 (2.4%)	$p = 1.000$
Online grooming:	10 (1.8%)	0	10 (2.2%)	$p = .378$

The internet is used to trick, force or pressure a young person into doing something sexual (e.g., sending an explicit video or image).				
Outing: *Private information is shared publicly without the victim's consent.*	4 (.7%)	1 (1.1%)	3 (.6%)	p = .506
Online reporting: *Misinformation about the victim is spread. Intends to harass or damage the victim's reputation.*	1 (.2%)	0	1 (.2%)	p = 1.000
Extortion	**218 (39.3%)**	**25 (28.1%)**	**190 (41%)**	**$t(131) = -2.44$, p = .016, Cohen's d = .27**
Webcam Blackmail Sextortion: *The victim is tricked into performing a sexual act on camera. This act is recorded and the victim is blackmailed to not share the recording online.*	134 (24.1%)	14 (15.7%)	119 (25.7%)	$\chi2(1, N = 552) = 4.06$, p = .044, Phi = .086
Content for ransom: *Sensitive information about the victim (e.g., images, secrets) is obtained and a ransom is asked for to not share the information online.*	60 (10.8%)	5 (5.6%)	53 (11.4%)	$\chi2(1, N = 552) = 2.70$, p = .101
Image based sexual abuse (aka Revenge porn):	24 (4.3%)	6 (6.7%)	18 (3.9%)	$\chi2(1, N = 552) = 1.46$, p = .227

Sexual images of the victim are shared online without consent.				
Unauthorised access	**44 (7.9%)**	**10 (11.2%)**	**34 (7.3%)**	***t*(112) = 1.09, *p* = .279**
Social media: *The perpetrator has accessed the victim's social media account without consent.*	17 (3.1%)	6 (6.7%)	11 (2.4%)	$\chi 2(1, N = 552) = 4.77$, $p = .029$, Phi = -.093
Email: *The perpetrator has accessed the victim's email account without consent.*	9 (1.6%)	2 (2.2%)	7 (1.5%)	$p = .643$
Via hacked Wi-Fi: *The perpetrator has accessed the victims home network.*	7 (1.3%)	2 (2.2%)	5 (1.1%)	$p = .315$
Via use of Bugs, Cameras and Trackers: *The perpetrator uses specific technology (e.g., listening devices, cameras) to surveil the victim.*	5 (.9%)	0	5 (1.1%)	$p = 1.000$
Virtual currency: *The perpetrator has accessed the victim's virtual currency without*	2 (.4%)	0	2 (.4%)	$p = 1.000$

consent.				
Gaming account: *The perpetrator has accessed the victim's online gaming account without consent.*	1 (.2%)	0	1 (.2%)	p = 1.000
Phone: *The perpetrator has accessed the victim's phone without consent.*	2 (.4%)	0	2 (.4%)	p = 1.000
Via use of phishing: *A malicious email sent to the victim that tricks them into sharing private information or downloading malicious software.*	1 (.2%)	0	1 (.2%)	p = 1.000
Physical device problem	**14 (2.5%)**	**5 (5.6%)**	**9 (1.9%)**	***t*(100) = 1.45, *p* = .151**
Malware generic: *The use of malicious software.*	12 (2.2%)	5 (5.6%)	7 (1.5%)	$\chi 2(1, N = 552) = 5.92, p = .015$, Phi = -.104
IT issue: *A non-cyber security issue. A wider issue with their technology.*	2 (.4%)	0	2 (.4%)	p = 1.000
Theft	**2 (.4%)**	**1 (1.1%)**	**1 (.2%)**	***t*(95) = .793, *p* = .430**
Fraud identity theft:	1 (.2%)	1 (1.1%)	0	p = .161

The victim's personal data is used fraudulently to obtain goods or services, often financially motivated.				
Website theft: *The victim's website is taken or withheld by the perpetrator.*	1 (.2%)	0	1 (.2%)	p = .161

Note. Total frequency refers to all 555 TFIPV cases examined between 17/12/18-23/03/21. Pre-COVID refers to cases of TFIPV from 22/03/19-22/03/20. Post-COVID refers to all cases of TFIPV from 23/03/20-23/03/21. Phi = .10 represents a small effect size, Phi = .30 represents a medium effect size, and Phi = .50 represents a large effect size (Cohen, 1988). Cohen's *d* can be interpreted as small (*d* = 0.2), medium (*d* = 0.5), and large (*d* = 0.8) (Cohen, 1988).

Did the Prevalence and Types of TFIPV Perpetrated Differ Pre and Post COVID-19 Restrictions?

The year prior to and post COVID-19 restrictions included a total of 552 TFIPV cases. Thus, three TFIPV cases were excluded as they fell before March 22, 2019. As noted above there was a substantial increase in cases post-COVID-19, with case numbers increasing from 89 to 463 cases. The substantial rise in cases unsurprisingly corresponds to increased frequencies for most of the TFIPV types. Therefore, to identify whether certain types of TFIPV were proportionally more common post-COVID-19 statistical tests were run.

Only one category differed significantly based on the time periods examined. *Extortion* was significantly more common post-COVID-19 than pre-COVID-19. Four individual TFIPV types differed significantly across the COVID-19 periods. Pre-COVID-19, three types of TFIPV were more common, *Cyberstalking, Unauthorised access to social media* and the *Generic use of malware*. Post-COVID-19, the use of web cameras for blackmail and sextortion was more common.

TFIPV Methods Employed

What is the Prevalence and Type of Methods used by Perpetrators to Commit TFIPV?

A total of 21 methods were used by perpetrators to engage in TFIPV. Figure 7 displays the definitions of each method along with an anonymised case example for illustration purposes. One additional method identified, but not used by perpetrators, is *Prevention*. Some of those who contacted the helpline were concerned that a current or former partner might be engaging in TFIPV, although they lacked evidence of a method, or might engage in TFIPV in the future. Although those victims and concerned persons who reported TFIPV reporters were

unable to identify a method of TFIPV, the helpline was able to assist these clients by helping them to implement preventative methods to secure their devices and profiles.

The 22 methods identified were used a total of 1195 times across the 555 cases of TFIPV examined. On average, each case of TFIPV involved two methods (*M* = 2.15; *SD* = 1.37), with a range of one to 10 methods per case. The frequency of method use is displayed in Table 6.

Given the large number of methods identified a decision was made to group similar methods to facilitate analysis. Methods were grouped based on the actions taken by the perpetrator to employ the method and the actions that would be required by the helpline to provide assistance to the victim. Figure 7 displays the five method groups and the individual methods included in those groups.

Figure 7: Method Groupings, Definitions and Examples

Group 1: Preventative

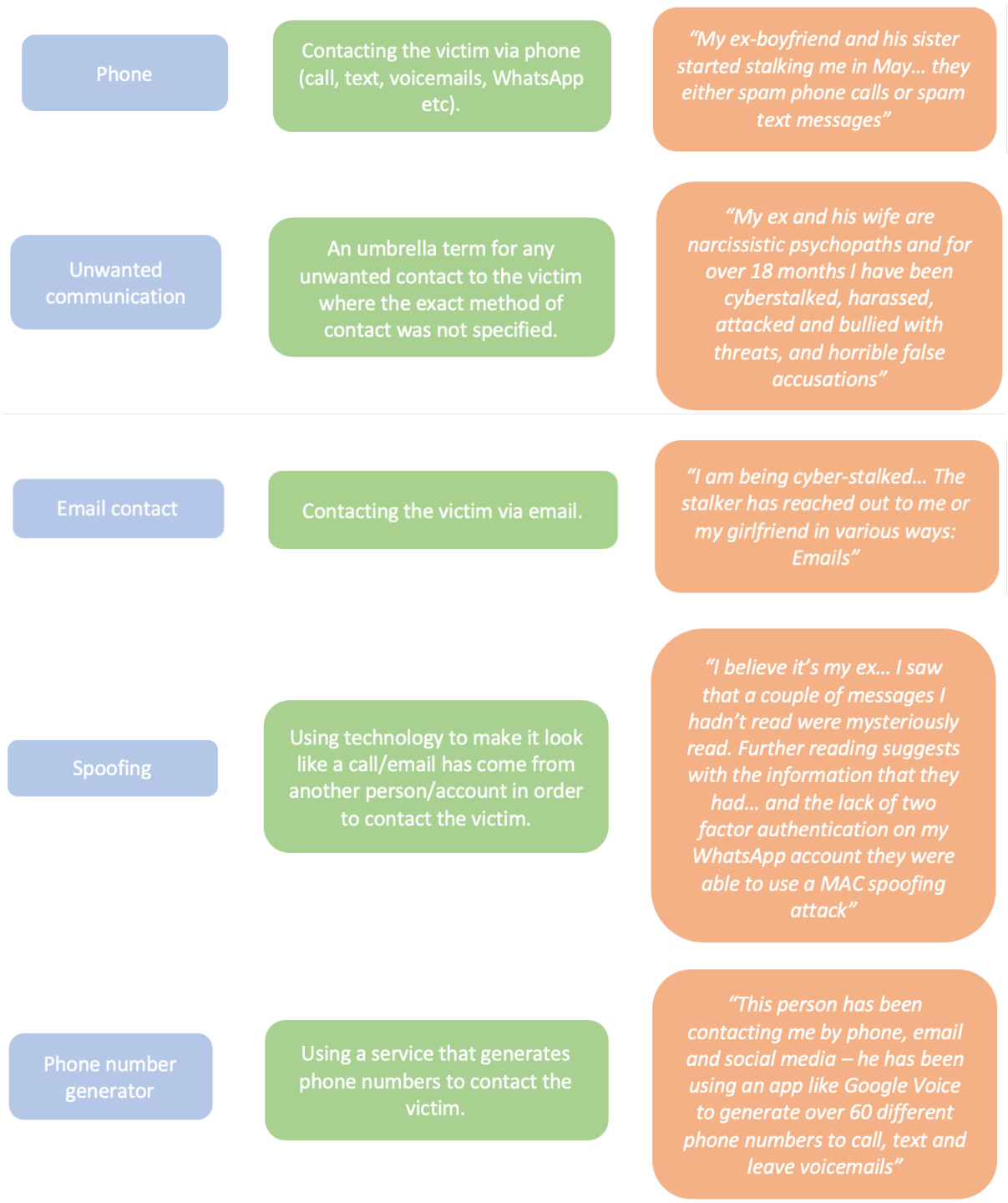
Group 1 includes only preventative methods, where the perpetrator's actions are unknown or unconfirmed, and the helpline engaged in various strategies to secure information and devices.

Method	Description	Example
Preventative method	There were concerns about the security of the victim's devices and online accounts, so the helpline assisted in securing those.	*"My ex-partner has been stalking me on Facebook… I want to know if there is a way I can check who looks at my Facebook account"*

Group 2: Communication with the victim

Group 2 includes methods where the perpetrator engaged in unwanted communication with the victim and the Helpline tended to advise that victims collect this evidence but not respond. In order of decreasing frequency these were: Social media, Fake profile, Phone, Unwanted communication, Email, Spoofing, and Phone number generator.

Method	Description	Example
Social media	Contacting the victim via social media.	*"I was chatting with a woman on snapchat and we were talking explicitly, and she screenshotted my explicit content and forced me to pay"*
Fake profile	Creating a profile(s) (e.g., social media) pretending to be someone else. This profile does not need to represent a real person.	*"I am being repeatedly stalked by my ex-boyfriend… I blocked him on everything, but he created fake profiles to try and add all of my social media"*



Group 3: Communication about the victim

Group 3 includes methods where the perpetrator posted or commented about the victim and the helpline advised on how to remove the content. In order of decreasing frequency these were: Videocall recording, Image based sexual abuse (aka revenge porn), Fake profile victim impersonation, Doxing, Website, Fake account, and Dark web.

Method	Description	Example
Videocall recording	Recording the content of a video call between themselves and the victim. Often used for blackmail or ransom purposes after the fact.	*"I met a girl on ____. We decided to text and skype call. On the call she got me to do sexual acts and is now threatening to upload it to my Facebook friends and family unless I send them money"*
Revenge porn method	Sharing or uploading sexually explicit/revealing images or videos of the victim without consent.	*"My ex-boyfriend sent private pictures of me to god knows who and now there is both a guy and a girl harassing me and sending those pictures and threatening to post them on a website"*
Fake profile victim impersonation	Creating a profile(s) (e.g., social media) pretending to be the victim.	*"I have an ex-boyfriend who... is creating fake dating profiles and other social media accounts and pretending to be me"*
Doxing	Releasing private and/or personal information about the victim publicly.	*"I was doxed by my ex, who was abusive to me"*
Website	Creating defamatory or fake websites about the victim; or used the victims' own websites to perpetrate abuse; or withheld the victims' own website.	*"Ex-partner is now trying to slander me online and destroy my reputation"*
Fake account	Signing the victim up for subscriptions or other online accounts (not including fake profiles).	*"My ex-partner... is pretending to be me, so... [has] been illegal[ly] putting government certification on my land registry"*
Dark web	Using the dark web to perpetrate abuse of the victim.	*"He's claimed that there are intimate photos of me on the dark web (8kun) and had threatened to share these with my workplace"*

Group 4: Technical surveillance

Group 4 includes methods that allow the perpetrator to track the victim's location, monitor who the victim is interacting with and to harass the victim. These methods may require specialised investigation or assistance from the helpline. In order of decreasing frequency these were: Hacking, Monitoring use of the internet, Spyware, Malware, Cameras, Bugs and Trackers, and Leveraging existing home smart technology.

Method	Description	Example
Remote access	Unauthorised remote access of the victim's devices, accounts, social media etc.	*"My ex-husband is possibly hacking my and my daughter's phone"*
Monitoring use of internet	Monitoring the victim's internet usage, including browsing, searches and websites accessed etc.	*"My ex-girlfriend stole my WiFi password and told me she's been invading my computer and watching my internet activity"*
Spyware	Software that is put, or used, on an existing device to spy on the victim.	*"My daughter feels that her husband… has linked his phone to hers so that he can read all her messages… [and] see where she is"*
Malware	Malicious software put onto the victim's device to steal information, access the device remotely or cause damage to the device.	*From the cyberstalking form* *"What stalking behaviours has the stalker shown so far? – Used malicious software against you"*
Cameras, bugs and trackers	External devices that are physically planted to watch, track or listen to the victim.	*"My husband is on bail for domestic abuse and put a tracker on my car"*
Leveraging existing home smart technology	Using existing devices or technology in the home to track, spy on, listen to or contact the victim. For example, Amazon's Alexa or baby monitors.	*"My WiFi router has been hacked by a girl I have been dating… My Alexa turned on playing a song on its own. She started manipulating Alexa while visiting me trying to make me think it was demonic and scare me"*

Group 5: Card fraud

Group 5 includes the method Card fraud alone for which perpetrators had to have bank details and the helpline's advice would be financially focused.

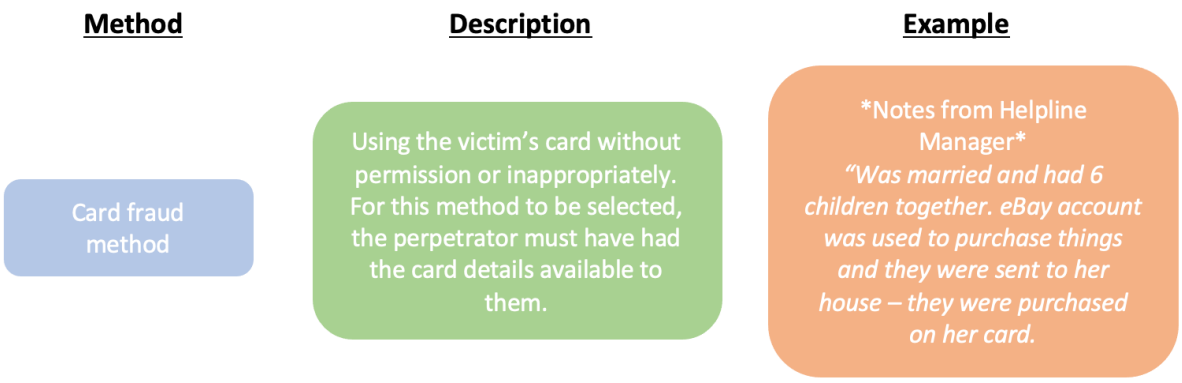


Table 6 presents the frequencies of method use at the group and individual levels. There was a high degree of variation in the overall frequency of method use. The group of methods related to *Communication with the victim* (Group 2) were the most common, although groups did not have equal numbers of methods. The use of social media to communicate with the victim was the most common individual method, followed by *Hacking* and the use of a *Fake profile* to impersonate someone other than the victim.

Information was gathered on the type of social media used to engage in the methods of TFIPV. *Social media* was used as a method in 171 (30.8%) of the TFIPV cases. An example of reported use is "the person… recorded it [the naked video] and uploaded it on Instagram". Multiple platforms were used in 34 (20.6%) of those cases. When individual platforms were used in the 165 cases the most common was Facebook (n = 67, 40.6%) followed by Instagram (n = 35, 21.2%), Snapchat (n = 16, 9.7%), Facebook Messenger (n = 10, 6.1%), LinkedIn (n = 2, 1.2%) and TikTok (n = 1, .6%). Social media contact was also recorded as public or via direct message. Most commonly, it was unclear whether the use of social media had been public or private (n = 100, 58.5%). Where discernible, social media use was most commonly via direct message (n = 52, 30.4%), followed by public (n = 14, 8.2%) and both public and private (n = 5, 2.9%).

Independent-measures t-tests were conducted to determine if there were differences between the method groups used by perpetrators who had been in brief versus longer term relationships with their victims. Current relationships were again excluded from these analyses as relationship length was unavailable. There was a significant difference for method group 2, $t(486) = 2.99$, $p = .003$, Cohen's $d = .26$, with methods involving *Communication with the victim* occurring more frequently following a brief ($M = 1.19$, $SD = .69$) than a long-term relationship ($M = .96$, $SD = 1.10$). There was also a significant difference for method group 3, $t(467) = 7.81$, $p < .001$, Cohen's $d = .70$, with *Communication about the victim* also occurring more frequently following a brief ($M = .61$, $SD = .58$) than a long-term relationship ($M = .22$, $SD = .53$). There was no significant difference for method group 4, *Technical surveillance*, $t(180) = 1.49$, $p = .139$).

Table 6. TFIPV Method Frequency and Comparison Pre and Post COVID-19.

Method	***n* (%)**			***Test of significance (χ or t-test)***
	Total	**Pre-COVID**	**Post-COVID**	
Preventative	-	-	-	-
Preventative	23 (4.1%)	6 (6.7%)	17 (3.7%)	$\chi 2(1, N = 552) = 1.76$, $p = .184$
Communication with the victim	**405 (73%)**	**49 (55.1%)**	**353 (72.2%)**	***t*(550) = 3.21, *p* = .001, Cohen's *d* = .36**
Social Media	171 (30.8%)	15 (16.9%)	155 (33.5%)	$\chi 2$ (1, N = 552) = 9.68, $p = .002$, Phi = .132
Fake Profile	138 (24.9%)	14 (15.7%)	123 (26.6%)	$\chi 2$ (1, N = 552) = 4.70, $p = .030$, Phi = .092
Phone	121 (21.8%)	12 (13.5%)	108 (23.3%)	$\chi 2$ (1, N = 552) = 4.25, $p = .039$, Phi = .088
Unwanted Communication	118 (21.3%)	17 (19.1%)	100 (21.6%)	$\chi 2$ (1, N = 552) = .279, $p = .598$
Email Contact	35 (6.3%)	11 (12.4%)	24 (5.2%)	$\chi 2(1, N = 552) = 6.47$, $p = .011$, Phi = -1.08
Spoofing	7 (1.3%)	0	7 (1.5%)	$p = .605$
Phone Number Generator	4 (0.7%)	1 (1.1%)	3 (0.6%)	$p = .506$
Communication about the victim	**181 (32.6%)**	**16 (18%)**	**164 (35.4%)**	***t*(163) = 4, *p* < .001, Cohen's *d* = .41**
Video Call Recording	118 (21.3%)	9 (10.1%)	108 (23.3%)	$\chi 2$ (1, N = 552) = 7.80, $p = .005$, Phi = .119
Revenge Porn Method	38 (6.8%)	6 (6.7%)	32 (6.9%)	$\chi 2$ (1, N = 552) = .003, $p = .954$
Fake Profile Victim Impersonation	17 (3.1%)	1 (1.1%)	16 (3.5%)	$p = .332$
Doxing	14 (2.5%)	0	14 (3%)	$p = .141$

Website	9 (1.6%)	0	9 (1.9%)	p = .367
Fake Account	6 (1.1%)	1 (1.1%)	5 (1.1%)	p = 1.000
Dark Web	2 (0.4%)	0	2 (0.4%)	p = 1.000
Technical surveillance	**188 (33.9%)**	**51 (57.3%)**	**137 (30%)**	***t*(186) = 1.25, *p* = .212**
Remote Access	156 (28.1%)	42 (47.2%)	114 (24.6%)	χ2(1, N = 552) = 18.76, p < .001, Phi = -.184
Monitoring Use of Internet	59 (10.6%)	21 (23.6%)	38 (8.2%)	χ2 (1, N = 552) = 18.52, p < .001, Phi = -.183
Spyware	42 (7.6%)	12 (13.5%)	30 (6.5%)	χ2 (1, N = 552) = 5.21, p = .022, Phi = -.097
Malware	40 (7.2%)	11 (12.4%)	29 (6.3%)	χ2 (1, N = 552) = 4.13, p = .042, Phi = -.086
Cameras, Bugs and Trackers	39 (7%)	14 (15.7%)	25 (5.4%)	χ2 (1, N = 552) = 12.13, p < .001, Phi = -.148
Leveraging Existing Home Smart Technology	33 (5.9%)	9 (10.1%)	24 (5.2%)	χ2 (1, N = 552) = 3.23, p = .072
Card Fraud	-	-	-	-
Card Fraud Method	5 (0.9%)	1 (1.1%)	4 (0.9%)	p = .586
Total	**1195**	**203**	**987**	***t*(550) = .938, *p* = .349**

Note. Multiple methods could be used in cases so total methods do not equal 555. Total frequency refers to all 555 TFIPV cases examined between 17/12/18-23/03/21. Pre-COVID refers to cases of TFIPV from 22/03/19-22/03/20. Post-COVID refers to all cases of TFIPV from 23/03/20-23/03/21. Phi = .10 represents a small effect size, Phi = .30 represents a medium effect size, and Phi = .50 represents a large effect size (Cohen, 1988). Cohen's d can be interpreted as small (d = 0.2), medium (d = 0.5), and large (d = 0.8) (Cohen, 1988).

Did the Prevalence and Type of Methods used Differ for TFIPV Cases Pre and Post COVID-19 Restrictions?

The methods used to perpetrate TFIPV were compared in the 89 cases that occurred in the year preceding the COVID-19 restrictions and the 463 cases that occurred post-COVID-19 (see Table 6). As above, given the substantial rise in cases post-COVID-19 the comparison of cases

pre and post-COVID-19 was run by doing a test of proportions to control for this rise and identify significant changes in method use.

At the group level, two significant differences were identified. *Communication with the victim* through the methods identified increased significantly post-COVID-19. Similarly, *Communication about the victim* increased significantly post-COVID-19. Both increases had small-medium effect sizes. No significant differences were identified across the two time periods in the other three groups.

Just under half (*n* = 10, 45.5%) of the individual methods showed significant variation pre and post-COVID-19. Pre-COVID-19 methods including *Email contact, Remote access, Monitoring internet use, Spyware, Malware* and *Cameras, bugs and trackers* were significantly more common. Post-COVID-19 period *Social media, Phone, Fake profile and Video call recording* were significantly more common. Effect sizes were generally small with the exception of *Email contact* which was large.

Discussion

Sample Characteristics

The results showed a clear and marked increase in TFIPV cases post-COVID-19. Although increases in reported abuse have been identified by other organisations, such as the 50-70% increase (Women's Safety New South Wales, 2020), the 420% increase seen by The Cyber Helpline is comparatively substantial. Relative to forms of offline IPV, TFIPV may have increased substantially because the lockdown forced more potential victims and perpetrators online, resulting in victims sharing more information and spending more time online and perpetrators having to devise new methods of engaging in abuse using technology. Thus, the increase in abuse may reflect a move to online methods by perpetrators who would have otherwise engaged in offline abuse.

Sample characteristics reflected previous research in some ways and not in others. TFIPV was more often perpetrated by males against females which is commonly found in IPV research. Victims were predominantly adults, which contrasts much of the available research on online abuse which has focused on adolescents (see question 3 in the REA). This difference may reflect the sampling methods of previous studies, where convenience samples at universities were used or where adolescents were targeted as participants due to heightened time spent online. Alternatively, our sample may reflect the fact that younger victims are not reporting abuse and seeking help to services like The Cyber Helpline or that they are obtaining help in other ways, such as through school. Given that referrals are made to The Cyber Helpline from multiple sources, including police, it is possible that younger victims are not receiving sufficient support from formal services specialised in TFIPV. This suggests that more awareness raising may be necessary among adolescents to direct them to specialised help and support.

Missing data were prevalent for several of the characteristics collected in the sample. This limits our ability to draw conclusions and run further comparative analyses to identify

differences in characteristics based on the types of abuse perpetrated and the methods used. Given the online nature of The Cyber Helpline's reporting and recording system, missing data is to be expected since obtaining this information it is reliant on victim reports and also victim knowledge of perpetrator characteristics, herein, victims had most often never met the perpetrator face-to-face. Where possible, future research designs that collect such information, perhaps through victim contact, would be beneficial to further characterise cases. The information gathered in such research may have implications for prevention and perpetrator treatment and management (e.g., the identification of personal problems that could be treatment targets).

TFIPV Type

Although much public discourse and concern about being online centres around theft and highly technical attack types, the present sample demonstrates that in the context of TFIPV these concerns are misplaced. The primary means of attack used by perpetrators were *Unwanted contact and communication* such as *cyberstalking, catfishing and harassment* and *Extortion*, primarily through recording videos and images of victims in conversation with the perpetrator or through the misuse of images/videos sent during a relationship.

These attack types reflect the sample examined herein, where there was a romantic relationship between the perpetrator and the victim. In the context of communication, this reflects a common characteristic of IPV and stalking where the perpetrator continues communication to force an ongoing interaction, rather than end the relationship, and/or engages in contact to exact revenge for what they view as a perceived slight by the victim. In the context of *Extortion*, perpetrators used intimate knowledge or intimate online relations between themselves and the victims (captured with or without consent) to demand something from the victim.

Notable differences in types of TFIPV perpetrated were found based on relationship type as well as pre and post-COVID-19. *Extortion* was more common in brief relationships, while *Unwanted contact and communication* and *Unauthorised access* were more common in longer term partnerships. This finding could reflect the fact that some perpetrators were entering brief relationships with the goal of obtaining material from the victim in order to extort them. As above, perpetrators in longer term relationships may be using *Unwanted contact and communication* to extend their contact with victims and/or punish them for perceived wrongdoing. The more common use of *Unauthorised access* in longer term relationships may reflect the fact that perpetrators have more access to the victims' devices or passwords or personal information allowing them to guess passwords.

The results suggest that education aimed at potential victims could be targeted based on relationship type. For instance, those in brief relationships could be targeted with warnings about the images they share and the intimate behaviours that they engage in online which could be recorded. For those in longer term relationships, education could focus on the access that partners have to devices, apps and passwords as well as the negative general consequences of relationship breakdown like stalking.

The TFIPV type category of *Extortion* was significantly more common post-COVID-19 due to a significant increase in the use of web cameras for blackmail and sextortion. There are several

possible reasons for this post lockdown increase. First, this may reflect the fact that as people moved more online during lockdown, opportunistic perpetrators took advantage of the change. Decreased romantic in-person contact with others as well as increased use of adult content online while working from home (Zattoni et al., 2020) likely drove more individuals to engage in sexual behaviour online when they would have otherwise done so in person. Opportunistic perpetrators could then have taken advantage of this increase in online sexual behaviour by recording the activities without consent and extorting victims.

Pre-lockdown, the attack types of *Cyberstalking, Unauthorised access to social media* and the *Generic use of malware* were more prevalent. The proportional decrease in cyberstalking post-COVID-19 may have been related to decreased victim access to stalking services and a subsequent decrease in referrals by those services to The Cyber Helpline. The decrease during lockdown may also reflect reduced reporting by victims who were less fearful of cyberstalking that was only carried out online, rather than in combination with an offline component. The decrease in unauthorised access to social media and malware during lockdown may reflect the fact that perpetrators' use of these attack types had previously been facilitated by physical access to accounts, passwords and devices.

TFIPV Methods Employed

The TFIPV methods identified were varied in nature and frequency. Varying levels of technological skill were required to use the methods, but most commonly limited technological skill was required, as evidenced by the prevalence of communication through social media, phone and email contact. The use of social media was the most common method employed by perpetrators which supports calls for additional safety provisions and platform accountability in managing online harm by social media organisations, app developers and technology companies (Messing et al, 2020; Harkin et al., 2020; Parkin et al., 2019; Parsons et al., 2019). Corresponding to the variation in method type are the varying types of assistance needed to counteract and record/retain evidence of abuse. This supports the need for specialised and trained interventionists like those comprising The Cyber Helpline. Novel methods of TFIPV were not identified. However, novel findings related to relationship type and the pandemic suggest ways to protect victims and reduce future TFIPV.

Perpetrators in brief relationships were more likely to use methods that involved communicating with or about the victim. Based on the categorisation of methods this likely represents the heightened use of extortion by this group. Specifically, where perpetrators communicated with victims to record video, obtain images and then make demands (i.e., blackmail) and then subsequently communicated about the victim by posting or sending the victim's personal information to others.

There were notable changes in the methods used by perpetrators pre and post COVID-19. At the group level, *Communication with* and *Communication about the victim* increased post-COVID-19. At the individual method level this corresponded to increases in communication via *Social media, Phone, Fake profile* and *Video call recording*. These changes align with the increase in *Extortion* as a type of TFIPV seen post-COVID-19.

Pre-COVID-19 methods including *Email contact, Remote access, Monitoring internet use, Spyware, Malware* and *Cameras, bugs and trackers* were significantly more common. There are several potential reasons for this variation. First, some of these methods are more technically complex than those that were used more frequently post-COVID-19. This may reflect the fact that pre-COVID-19 perpetrators who engaged in TFIPV did so as a first choice based on their technological expertise/experience, while post-COVID-19 perpetrators who engaged in TFIPV did so out of necessity due to a lack of contact with victims and thus used less complex methods given their more limited skill sets. Second, the lockdown increased the time that individuals spent online, and by default increased the information they volunteered online as well as normalised certain practices (e.g., video calls over phone calls, sexual encounters via video call). This behaviour change increased the opportunities available to perpetrators to exploit this activity in simple ways for use in TFIPV. Pre-COVID-19 perpetrators may have therefore needed to use more complex and surveillance-based methods to access and uncover the same level of information which was more freely available during the lockdown period. Third, some of the methods more commonly used pre-COVID-19 require a degree of physical access and groundwork (e.g., installation of cameras, bugs and trackers) that would have been less available during lockdown.

Strengths and Limitations

The results should be interpreted in consideration of project limitations. First, during the time period examined there were changes in how The Cyber Helpline collected and managed victim data. Prior to the implementation of the Helpdesk in August 2020, cases with Helpline Responder involvement were primarily managed and resolved through email. This meant that case information was sometimes limited, and case communications were not stored collectively as a single case file. The introduction of the Helpdesk meant all case information and communications with a single victim were stored in one location as a unique file. Consequently, cases in the Helpdesk had more detailed and complete information which may have an impact on pre- and post-COVID-19 comparisons.

These changes are to be expected in an area like online harm which is constantly evolving. Further, the impact of these changes on the data available for the study was mitigated by The Cyber Helpline in several ways. The Cyber Helpline met an over 400% increase in demand with creative solutions such as the Helpdesk to manage caseload and communication. The Cyber Helpline were supportive throughout the data collection and coding process and made all case information available for examination by the RAs and consulted as necessary to ensure thorough and accurate coding. Coding across cases was also consistent with highly trained coders and review of all cases by two coders with consensus discussions where necessary with the PI and The Cyber Helpline. Research on online harm is a developing area and as our understanding of this issue increases, our ability to consistently collect and code data will also improve. Types and methods of online harm are constantly changing; thus, research must do its best to remain current and abreast of the emerging issues. Research examining online harm must always be on the cutting edge.

A second potential limitation is that, for coding purposes, we chose to record all victim reporting as accurate. This was considered as the best approach as there were no sources of corroboration, and is often the approach taken in other file review studies. However, it is

acknowledged that victim reports may have been inaccurate, or influenced by social desirability factors. The nature of online relationships and communications means that it is not always easy to verify the identity of the individual you are engaging with. In cases of catfishing, for example, it is difficult to determine the actual gender of the perpetrator. Victims also often reported the online behaviour in a way that minimised their level of engagement with the perpetrator: for example, there were several cases of webcam blackmail whereby the victim was engaging in online sexual behaviour with someone other than their current partner but reported only observing online sexual behaviour. In these cases, it was apparent based on extortion threats that the victim was most likely cheating on their partner but was attempting to minimise their involvement.

Despite the potential issues associated with relying on victim reports, all cases were coded consistently as noted above. The RAs were supported throughout coding by a coding tool, which was informed by the expertise of academics and the Helpline. The coding tool was also adapted through several coding trials to ensure that all identified TFIPV attack types and methods were accurately reflected in the coding sheet.

A final limitation is that this research project was exploratory in nature and multiple comparisons were conducted via various statistical analyses. When conducting multiple comparisons in research, the risk of a Type 1 error (the error of a false positive) increases. Caution must therefore be taken in the interpretation of the results.

Beyond the limitations outlined above, there are also several strengths to this project. As discussed previously, this project examined a current and evolving issue, thus contributing to our understanding of TFIPV and online harm. The project was informed by individuals with a range of academic and field expertise, and the RAs were all PhD level raters with experience and training in data coding. The project involved a large and representative sample with a review of all online harm cases reported to The Cyber Helpline in a 27-month period. The project also enabled researchers to examine and compare online harm behaviours during an unprecedented pandemic, with COVID-19 providing a unique opportunity to examine the impact of lockdowns and other restrictions on online harm and TFIPV specifically. Results revealed unique impacts of the pandemic on TFIPV prevalence, type and method.

Workstream 3: Synthesised Data Collection from The Cyber Helpline Responders

Introduction

Research into practitioners' experiences of working with victims of offline intimate partner violence (IPV) vastly outweighs that which focuses on victims of online IPV. This remains true despite research indicating the significant likelihood of practitioners encountering victims who have experienced online forms of IPV. For example, Woodlock et al. (2020) discovered that almost all (98%) of the practitioners in their study had worked with clients who had experienced online IPV, such as threats to distribute intimate images (49%), excessive texting (47%), and harassment via social networking systems (37%). The growing recognition technology-facilitated intimate partner violence (TFIPV) has prompted a call for more guidance for practitioners to assist in effectively recognising and responding to TFIPV, while meeting victims' increasingly complex online safeguarding needs (Harris & Woodlock, 2019; Douglas, Harris, & Dragiewicz, 2019; Powell & Henry, 2018).

However, much less focus has been paid to the experiences of cyber specialist practitioners who regularly engage with victims of TFIPV. Therefore, to better understand these dynamics, data was obtained from several frontline responders at The Cyber Helpline to elicit insights about their experiences of supporting and safeguarding victims. The Cyber Helpline is a not-for-profit organisation that aids victims of cybercrime in the UK. It began operating in May 2018. It was founded by Rory Innes who built a team of volunteers with significant experience in the cyber security domain to manage and run it, and it currently has 4 board members. Their aim is to "ensure that everyone in the UK has immediate access to expert cyber security help when they need it" and their delivery model is to "help individuals understand, contain, recover and learn from cyber-attacks by linking them with cyber security technology & experts who provide relevant advice and guidance" (https://www.thecyberhelpline.com/team).

A three-phase, staggered approach was employed to obtain the required stakeholder information. An outline of this, along with the relevant research questions pertaining to each phase, is presented below:

Phase 1) *Written Responses*: Members of The Cyber Helpline who had indicated their willingness to take part in a semi-structured interview (phase 2) were emailed the two TFIPV victim-oriented research questions (RQ1 & RQ2) which focused on understanding risk assessment practices and specialised support provided by the charity. The analysis of the written responses generated from this communication forms the first part (Part 1) of the findings section.

RQ1. How does The Cyber Helpline Perform Risk Assessment for Victims of TFIPV?

RQ2. What Support Practices do The Cyber Helpline Provide to Victims of TFIPV?

Phase 2) *Semi-Structured Interviews*: Several members of The Cyber Helpline indicated their willingness to take part in a semi-structured interview focusing on TFIPV, and the interpersonal nature of such harm. The analysis of their responses to the three perpetrator-oriented research questions (RQ3, RQ4 & RQ5), which focused on types of TFIPV behaviours encountered, current factors impeding effective action against TFIPV, and recommendations for interventions to tackle TFIPV, forms the second part (Part 2) of the findings section.

RQ3. What are the Technology Methods Employed by Perpetrators of TFIPV?

RQ4. What are the Factors Impeding the Response to TFIPV?

RQ5. What are the Recommended Interventions to Tackle TFIPV?

Phase 3) *Online Survey*: Members of The Cyber Helpline volunteers' network were invited to complete an online survey which was informed by a preliminary analysis of the data obtained in phases 1 and 2. Survey respondents indicated their perceptions of supporting victims of TFIPV, with a specific focus paid to the nature and extent of victims' (digital) vulnerabilities; current technological factors and gaps informing or impeding TFIPV perpetration; and the feasibility of proposed TFIPV technical, legal and social interventions, addressing above mentioned research questions RQ4 & RQ5 as well as RQ6. The analysis of their responses forms the third part (Part 3) of the findings section.

RQ6. What is the digital susceptibility of victims to TFIPV?

Methodology

The data collection instruments all underwent full ethical scrutiny and were approved by the School of Psychology's Ethics Committee prior to the commencement of the project. All participants across the three data collection phases were sourced from The Cyber Helpline with the assistance of the Helpline Manager.

Method: Written Responses

Thirteen members of The Cyber Helpline who indicated that they were willing to take part in interviews were emailed to provide written insight into their working practices concerning risk assessments of TFIPV victims, and to outline the support practices in place for these clients, addressing RQ1 and RQ2. Eight of the thirteen participants returned written responses to these two questions; they are identified in Table 1 with a * symbol in the gender column. To avoid duplication, further details about these thirteen participants can be found in the 'semi-structured interviews' section.

Method: Semi-Structured Interviews

Sample

The Helpline Manager provided the contact details of 17 Helpline Responders who expressed willingness to participate in the research. The Helpline Responders were sent an email detailing the goal of project, the nature of the project and the financial remuneration on offer for taking part in an interview. Thirteen current or former workers/volunteers for The Cyber Helpline indicated their willingness to participate in interviews. These respondents were sent a Qualtrics web link to access an information sheet detailing study aims, withdrawal of participation and the deadline for doing so. The link also contained a consent form. Eleven participants returned the consent form prior to the interview. The remaining 2 participants, who did not submit their consent form in advance, provided verbal consent at the beginning of their interviews. Of the 13 participants, 10 were men and 3 were women. Table 7 provides an overview of the interview participants and their experience.

Table 7. Characteristics of The Cyber Helpline Responder interview participants.

Gender	Length of Time Working at The Cyber Helpline	Working in the Pandemic?	Length of Time Working with Victims of Cybercrime
Female *	2 years	Throughout the pandemic	2 years
Male	14 months (no longer there)	Before and during the pandemic	4 years
Male *	Just over a year (no longer there)	Pre-pandemic	1 year (only at The Cyber Helpline)
Female	Just over a year	Before and throughout the pandemic	6 years (including work at The Cyber Helpline)
Female *	8/ 9 months	During pandemic	8/9 months
Male	17 months	Throughout the pandemic	17 months
Male	1.5 years (ex-employee, takes breaks from employment but still helps out)	Before and during the pandemic – ceased in July	2.5 years
Male *	5 months	During the pandemic	5 months
Male	Almost 1 year	During the pandemic	2.5 years

Male *	4 years	Throughout the pandemic	8/9 years
Male *	2 years	Before and during the pandemic	2 years
Male *	1 year	During the pandemic – started roughly two months after first lockdown	1 year
Male *	15 months	Throughout the pandemic	15 months

Although several participants were new to supporting victims of cybercrime when they first joined The Cyber Helpline, many came from a background of cyber security (e.g., from educational or work experience). For example, one participant discussed their previous role within the cyber security field, noting the differences they had observed between the corporate and not-for-profit sectors (they said: "*The Cyber Helpline has an individual/victim focus, and specifically deals with non-corporate victims*"). Another participant had previously worked in multiple investigatory roles within the videogame industry and Internet Watch Foundation (e.g., assisting in evidence gathering and researching patterns in online grooming) and was currently the research and development director at a cybersecurity company. Another participant managed a company that assists organisations and specialises in cyber security. This was the case for several helpline responders; although they had cyber security experience, prior to joining The Cyber Helpline much of their work had been in the corporate sector, rather than the charitable or not-for-profit sector. The range of experience and expertise provided by The Cyber Helpline responders demonstrates the skilled and varied pool from which the participants were sampled.

Data Collection

Two research assistants (RAs) from the University of Kent conducted all 13 interviews via MS Teams between 14 and 21 April 2021. Participants were invited to turn their cameras off prior to starting the interview recording. The MS Teams transcription facility was employed to generate transcripts of the interviews automatically. These transcripts were safely stored as separate MS Word documents before being aggregated into a master transcript document (422 pages) to be checked for accuracy against the recording and amended accordingly. The interviews lasted approximately one hour each.

Data Analysis

The two researchers (Co-I Franqueira and Co-I Duggan) and three RAs undertook a thematic analysis of the master transcript. Co-I Franqueira and two RAs research assistants independently coded the master transcript. All five researchers assessed these codes. Co-I Duggan and two RAs generated themes using these codes.

Method: Online Survey

Survey Design

The survey was organised in four-parts. The first three parts provided a total of 73-statements, informed by a preliminary analysis of the data obtained in phases 1 and 2. Participants were asked to rate the statements using a 5-point Likert scale (1= 'strongly disagree' to 5= 'strongly agree'). At the end of each part, a free-text box gave participants the opportunity to add information that was pertinent to the research question but had not been covered in any of the statements, participants could also rate this additional information on the same 5-point Likert scale.

The first part of the survey addressed RQ6. Participants were presented with 22 statements representing victim vulnerabilities and were asked to rate the frequency (from 'never' to 'always') of victims' digital vulnerabilities that are exploited by perpetrators, according to their experience in supporting victims of TFIPV.

The second part of the survey addressed RQ4 and was divided into two sub-parts: technology and non-technology related gaps in countering TFIPV. The first sub-part explored participants' level of agreement (from 'strongly disagree' to 'strongly agree') with 9 technology-related gaps in countering TFIPV, while the second sub-part explored their agreement with 22 non-technology related gaps in countering TFIPV.

The third part of the survey addressed RQ5, which focused on the recommended interventions to tackle TFIPV. Participants were presented with 20 statements representing potential interventions and were asked to rate their level of agreement with proposed interventions to tackle TFIPV.

The final part of the survey was an open-ended question allowing participants to add any further comments.

Sample

The online Qualtrics survey link was distributed to 46 current and former workers/volunteers of The Cyber Helpline by the Helpline Manager. It remained active from 29 April to 12 May 2021 and four reminders were sent via email. There was a total of 26 responses recorded in Qualtrics. After excluding blank and partial entries, there were 16 complete responses to the survey. Due to the small sample size, only descriptive statistics are presented in the findings.

FINDINGS

Part 1: Written Responses

All thirteen participants who indicated that they were willing to take part in interviews were emailed to provide written insight into their working practices concerning risk assessments of TFIPV victims, and to outline the support practices in place for these clients. An analysis of these two areas, addressing research questions RQ1 and RQ2, as determined from the seven returned responses is detailed below.

Risk Assessment Practices

The Cyber Helpline uses a staged approach to assess whether victims are in imminent risk. The first layer of assessment is performed using a chatbot (e.g., online robot-based chat), accessed via the charity's website. If the chatbot identifies imminent risk, victims are directed to call 999 themselves:

> *… our chatbot… allows someone to seek help anonymously without a chain of communication*

The chatbot performs a triage by identifying the type of cybercrime or cyber-attack the victim is experiencing based on information provided. If the victim states that they would like to have assistance from one of the charity's responders, the chatbot collects contact details and alerts responders on call.

The second, two-step layer of risk assessment is undertaken for certain types of cybercrime, such as cyberstalking and domestic abuse cases. First, an "online footprint form" is completed, e.g., understanding the victim's online presence, technologies used, digital/online practices, and technical skills. Second, a "cyber stalking action plan form" (also called a "stage two form") is compiled; this details the perpetrator's behaviour towards the victim, and the impact caused by the perpetrator to the victim.

The information from both forms allows the helpline responder to gauge the risk posed by the perpetrator, as well as the victim's level of digital and physical vulnerability. Furthermore, the information not only indicates to the charity the level and type of support required for safeguarding the victim—particularly in terms of technology and the collection of evidence—but also feeds into decisions regarding the referral of victims to an external risk assessor, (e.g., domestic abuse specialist, or the police):

> *For risk assessment, we give the victims an online footprint form and a stalking form to fill out and that helps us in understanding the risk the victim is at.*
>
> *This [using both forms] allows us to get an internal feel for red flags - and a rough picture of risk - so we can assign internally and signpost where needed.*
>
> *In some circumstances, we may also make referrals with their [the victim's] consent to other organisations, such as domestic abuse organisations, and may also advocate with the police on their behalf.*

The charity has an internal process for escalation of concerns where responders can flag risks that were noticed in a case:

> *We use a vulnerable users policy in order to ensure that we are speaking to someone of a certain age and to ensure they don't feel in any immediate danger.*
>
> *… there was a system in place where incidents or concerns could be escalated. The Helpline has a support structure in place, so any concerns that a Responder may have could be discussed with the Helpline Manager or one of the Directors.*

It was also noted that all volunteers undergo training before becoming official responders. The range of training includes not only the process of assistance, but also identification of risks and escalation:

> *The training completed by all Responders covered, in detail, what would constitute a vulnerable user… The senior/experienced staff, as well as the Helpline Manager and Directors, at the Helpline would provide assistance where required.*
>
> *Our team are trained on risk assessment methodology, but we prefer to have an external expert risk assess.*

In terms of risk assessment and vulnerability, it was noted that The Cyber Helpline provides cyber-related support for anyone aged 13 or over. However, the charity responders are only authorised to handle cases for victims who are adults (18 or over). Cases involving victims aged between 13 and 17 years old must adhere to the charity's "Vulnerable User Policy" that dictates that they should be handled by a Director or a trained Senior Helpline Responder.

Providing Support

The Cyber Helpline provides technical assistance to victims of cybercrime in four main ways, namely, (1) assistance to understand technology-related vulnerabilities and how they are—or can be—exploited by the perpetrator in question, (2) assistance to secure their devices, online accounts, and home against the perpetrator, (3) assistance to gather digital evidence for a potential (legal) action against the perpetrator, and (4) assistance to learn best practices to keep safe and prevent similar cases in the future:

> *We help the victim understand how technology is being used and demystify any confusion around the technology… We essentially act as a cyber security expert helping them deal with the technology components of their case*.

Responders highlighted the need for flexibility when supporting victims. Examples included recognising the need for varying communication channels to better accommodate victims' circumstances, keeping in touch with victims, and offering an "open door" policy that allow victims to interact with the charity as desired, on their own terms, following the culmination of their case:

> *… In terms of support, it is via e mail or by phone with analysis of their individual situations.*
>
> *… Secure communication channels (To help with private conversations or one time emails).*

> *We also make the victims aware that if they need further support they can always contact us again and we will reassess the situation.*
>
> *We would complete regular checks to see how they are getting on.*

The charity website provides a range of online guides where victims can find information—independently and anonymously—about how to deal with the issue experienced in terms of technology. As part of their service, the charity refers victims to other organisations that supply specific support, effectively complementing that which is provided by the charity:

> *We offer the victims the possibility to be referred to specialised charities to deal with the non cyber related issues.*
>
> *… links to a number of other sources which they [victims] can follow up with if necessary*
>
> *We provide our Guides and Assistance to secure their technical world. We also assist with sign posting to other charities or support teams for additional support such as mental health.*

In sum, the helpline responders indicated that they were trained to ensure they could competently identify and assess victims' levels of risk, provide a range of safeguarding and specialist advice, and had the relevant connections in place to ensure that they could signpost victims to relevant domestic abuse charities or other such agencies, as necessary. This information provided a useful platform from which to explore the participants' experiences of dealing with TFIPV perpetration, which forms the basis of the following section.

Part 2: Interviews

Interviews were conducted with helpline responders with a range of knowledge, expertise, length of service, and levels of seniority. These participants provided insight and information regarding the nature of TFIPV, obstacles to effectively challenge this, and avenues for future interventions aimed at recognising, responding to, and reducing TFIPV.

Technology Methods Used by TFIPV Perpetrators

The third research question (RQ3) aimed to explore the types and uses of technology by perpetrators. The emergent findings have been grouped into three main themes relating to methods employed by perpetrators: *leveraging opportunities*, *physical proximity* to victims, and *manipulating victims*.

Leveraging Opportunities

The nature and type of TFIPV perpetration has evolved in line with the growth in available technologies and online connectivity. The same technologies that have facilitated the shift to virtual work, education and social interactions (particularly post-COVID-19 restrictions) have also been instrumental in creating new opportunities and methods to perpetrate TFIPV.

Contrary to popular belief, most TFIPV is carried out via simple methods, which do not require perpetrators to have specialised knowledge or strong technical skills. Popular methods mentioned included access to victims' mobile phones, email accounts and social media accounts (especially Facebook), gained from knowledge of victims' passwords. Such unauthorised access was often referred to by Helpline Responders as "hacking". For this document, we regard "hacking" as unauthorised access regardless of how credentials were obtained.

Password access was facilitated through the victim having shared this information previously with perpetrators, having predictable passwords, or using the same password for multiple accounts. In other cases, perpetrators had forced the victim to share their password, or had accessed this information covertly by other means (e.g., watching as it was typed). Similarly, shared family accounts made keeping track of victims easier:

> *…a common password, again, that they're using or that's quite easy to guess, or that in some way they're receiving, they've got [the victims'] emails on their phones and they're able to do a password reset*

> *The most effective stuff is absolutely the everyday devices and accounts that their victims have… it's their email account. It's their social media accounts.*

> *You know they could use their email account, they can use their Facebook account, but they [perpetrators] don't have any more skills than that.*

Another popular method was to use GPS-enabled apps designed for legitimate purposes (e.g., tracking children's movements or locations, finding lost phones, checking friends' whereabouts) or spyware to keep track of victims without raising suspicion:

> *What we see a lot of is that people assume that it's spyware, but as we go along we find that it ends up being that it's, kind of a more simple explanation. So it tends to be the hacked [victims'] accounts that are the most common factor in that, or that they've [the perpetrator] set themselves up on Find my Friends or some sort of tracking app [on the victim's phone].*

> *They live together. They've got location sharing on… it's not uncommon between romantic partners to have location sharing on.*

> *We tend to find is that [perpetrators] try to find a way to watch their partners without them knowing, and one of the best ways that they do that is they kind of add spyware onto things like the router or the mobile because it's not obvious to the partner that the perpetrator's done this.*

Perpetrators leveraged a range of technologies which were readily available in the victim's home, were used by the victim's children, or had been pre-installed for safety or security reasons. For example, Helpline Responders noted that perpetrators were using smart devices and appliances (referred to as "home IoT", such as smart TV, smart lights, smart speakers), gaming consoles, and CCTV cameras for monitoring purposes or to intimidate victims:

> *What we've seen a lot more of recently is probably kind of, smart home side of things. So, you might see that cameras are being used to monitor when they're leaving the*

house or entering, and even down to a couple of cases where Alexa's been used to turn on and off the lights, or to turn on and off the TV, change the channel and things like that.

… [perpetrators] get into their sons' Xbox account and then utilize the Xbox… to watch what the children are doing and… feed that back to the ex-wife and scare her.

Alongside methods such as infecting the victim's devices with malware (e.g., for remote access), and using the router's (browser) interface to monitor connections to the home's wireless network, perpetrators also took advantage of more sophisticated or unusual ways to perpetrate TFIPV (albeit more rarely):

… sending the bank transactions to their bank account. So you send a payment of 1 Pence to the victim…. Just put the stalker's name or you make a threat in that little tiny… 30 letter [reference] box [for payment].

The emergence of the COVID-19 restrictions played a significant role in TFIPV perpetration and victimisation. In the UK, the 'stay home' lockdown order presented increased opportunities to leverage technology to perpetrate TFIPV. During the three UK lockdowns, daily activities (e.g., work, education, shopping) increasingly took place online, making it difficult for victims to try and stay offline:

What people in these situations typically did when they came to us is they had unplugged from technology. So they had… stopped using email… stopped using their device. They were kind of reverting back to an offline life and that was how they felt safe from online activity. That option just doesn't exist in lockdown. You know you need to order your food online. You need to order stuff online it's how you communicate and keep up to date with stuff.

The Helpline Responders noticed a higher volume of TFIPV cases, alongside an increase in abuse intensity:

It's not new tools for the perpetrator to use themselves as such, but there's more access for them because the victims are using so many more things online, it's just more kind of doors for them to try and open.

I don't [think] techniques changed, but I think it has got worse … definitely been a problem exacerbated.

… we saw people get more devices and bits of tech that they probably never dealt with.

While the lockdown periods rendered abuse more "cyber dependent", Helpline Responders reported that the type of technology used by perpetrators did not significantly change. Most perpetrators used available methods and means, but took advantage of the increased accessibility and availability of victims being online or knowingly at home:

It has forced people to remain online and therefore presented more of an opportunity for [perpetrators] to engage with the stalking behaviour or harassment behaviour.

> *I think the main pattern has been during COVID from all the data that I know from before, it's more the... cyber harassment cases that can potentially get into cyber stalking. They seem to increase every time we go into a lockdown. I think it might be because everybody is locked in the house and it's quite difficult to actually meet the person. If you're actually trying to do something.*

One notable method to emerge during lockdown was perpetrators sending victims deliveries of gifts or unwanted goods:

> *… just seeing more cases, so, more people under stress resorting to this kind of thing with ex-partners… more phone calls, text messages… some nice gifts… you know the Amazon guy turns up give you something, you realize it's from the stalker or the person, or… [a] threatening gift… something that either shocks or has a… negative impact.*

Perpetrators were presumed to have had more time for abusing (or for considering abuse) post-COVID-19. Coupled with the increased time spent online, this was seen as having informed their engagement in learning about, or committing, TFIPV:

> *… there is so much information out on the Internet that you could just Google search … "how to track my partner" if you put that into a search engine… it'll give you loads of different ideas on how to do it.*
>
> *[If not for lockdown] we probably wouldn't see [perpetrators] committing these acts because they probably wouldn't know how, but it's probably given them the time to, kind of, search online and figure out how to do these things, which they wouldn't otherwise do.*

Physical Proximity

Helpline Responders indicated that having physical access to the victim's home or personal devices enabled perpetrators to take advantage of the opportunity to commit some forms of TFIPV:

> *The most common thing I guess that we see is... that physical access has been present to allow them [the perpetrators] to do something with the phone physically or to be able to set it up for them [the victim] in the first place.*
>
> *If they [perpetrators] have physical access to the house, then they may be able to manipulate the wireless network. They may be able to manipulate the computers…*

Helpline Responders confirmed the significant role that technology has had regarding the changes in IPV perpetration, due to increased technological knowledge and accessibility:

> *I think it's the increase of technology …*
>
> *Being able to buy bugs, that I think potentially we might have seen an increase in bugs in the house and microphones and stuff like that.*

While it is possible to purchase surveillance devices online with few restrictions, these devices (or "bugs") require physical access for installation and may require maintenance for battery replacement and for changing data storage (e.g., SIM or SD card). Connecting these bugs directly to the mains power of the house eliminates the need for battery replacement:

> *Definitely a lot more of the tracking side of things and the bugs to facilitate that control... they're really easy to get them online for like 20 pounds.*
>
> *… what we see the most of, I'd say, is, kind of, plug sockets, extension cables, stuff like that that you're using constantly, but you don't think there's a SIM in that. You'd have to take it apart to find out.*
>
> *It's just something as simple as a mouse on a computer for example, because once you've plugged it into that USB slot it's getting a constant power source. All you have to do is put a SIM in there, and the SIM's constantly recording.*
>
> *… most of the time you have a battery… SD card in it [bug]. You put it on. If you still have access to the house, 2 weeks later you go take this SD card, plug it in the computer and listen.*

Having physical proximity to victims—combined with factors such as victims having a poor understanding or limited interest in technology—empowers perpetrators to remain the "technology expert" in the relationship. This imbalance (or perceived imbalance by victims) allows perpetrators to take over the installation and establishing of privacy settings for personal devices, home devices and accounts, leaving victims vulnerable to TFIPV:

> *Victims don't really have a massive grasp of technology, which is why their partners or ex-partners are setting up their accounts and devices for them.*

Perpetrators may link to the victim's device to facilitate access at a later stage. This can be done by confirming a previously unrecognised device as legitimate, giving users control of which devices can access their accounts. Once a device is recognised as "trusted" (when first used for access) it remains as such until it is manually removed from the list of trusted devices for the account. Since it is common practice among many people in romantic relationships to use each other's devices to access accounts, those usually become recognised as trusted devices. When the relationship goes wrong, if the victim does not remove unwanted trusted devices, the perpetrator will still have access to the victim's account:

> *… [the victim's] trusted a device or a person through that [iPhone] to allow them [the perpetrator] to watch or the person has access to their [the victim's] iCloud.*

Manipulating Victims

Helpline Responders outlined several different ways in which manipulation featured in the perpetration of TFIPV. This either related to acts undertaken by the perpetrator to manipulate the victim with the use of technology (e.g., to monitor and harass), or to facilitate the psychological manipulation of victims (e.g., coercion and gaslighting).

Perpetrators can create multiple fake accounts to access the victim, which has the effect of bypassing the victim's efforts to keep distance. Victims are often aware that the perpetrator can keep creating new accounts and continue with their campaign of persistent harassment. This was noted alongside the victim's recognition of being unable to prove it was the perpetrator behind the abuse.

A difference was noted between passive surveillance (as outlined above) and active manipulation with regards to TFIPV. While some perpetrators used their unauthorised access to spy on victims, others went a step further, deleting important documents files or email messages that pertained to issues like divorce, child custody or other disputes, or changing information on social media profiles. Perpetrators also had the ability to change the settings to lock victims out by altering the login details or disabling trusted devices. Information obtained from a victim's email inbox may be used to cause psychological distress where victims are unaware that the perpetrator has access to, and is manipulating, their email account:

> *[perpetrators] try to destroy evidence or tamper with communications, but it's usually because of a legal driver or money via divorce, ailment, or custody of the kids.*
>
> *… sometimes it's gas lighting and confusing… sort of. You know, things just get deleted… [the victim know] that there was an email. Though it's gone…*

Gaslighting arose in other examples of TFIPV cited by Helpline Responders, where the perpetrator's psychological manipulation caused victims considerable distress and feelings of persecution:

> *… if you sign into [the home router] it's normally got a piece of software that allows you to turn off certain devices at certain times of the day… aimed at children so that at 9:00 o'clock… it's bedtime [or] they can't go on the Internet on their phone... But again it can be used… in harassment cases to block people… [and] confuse them.*
>
> *He [the perpetrator] would send out conversations… that she [the victim] had with her [new] partner to other family members… private conversations. So, I think that had a massive impact because the victim didn't really feel like she could talk to anybody or trust technology…*

Examples also demonstrated the exhausting nature of TFIPV for victims, with perpetrators being both relentless and unpredictable in their online campaigns of harassment:

> *… a lot of the time they get so obsessed that they just constantly want any way of contacting [the victim] … where someone may have… blocked them on Facebook, block[ed] them on messaging, blocked them on email, blocked them on telephone and they just found another method to send a message to the person.*
>
> *… the control mechanism is really just fear through stalking itself… one of the… definition points of stalking legally is what impact does it have on [the victim's] day to day life… They have to completely change their lives, they have to stop socializing. They don't do school pick up anymore…*

Some forms of TFIPV were undertaken covertly, with efforts made by the perpetrator to evade detection where possible. This included installing bugs or monitoring software on victims' devices well in advance of a breakup, detailing the calculated and premeditated characteristic of some perpetrators:

> *it's also very easy for [perpetrators], especially if you're in a relationship, to have 5 minutes away with [the victim's] phone. Obviously you trust your partner at this time, and you don't know how quickly things go on where... If [perpetrators] plan ahead, and maybe they know something is going to happen in terms of going to break up and stuff, they'll probably be doing this a couple weeks back, couple of months back, before that before actually happens. And it because, people get a sense of how things are going, and if things are going the wrong way, they'll have that bit of leverage already before anything kind of even starts. And again, it all it takes is a fake Calculator app a fake kind of software, especially on these androids where nobody knows what all these bits do, and the fake software update that that kind of gets used. And then yeah, yeah, easy as that, really, especially if you still know their Google password at this point.*

For those who wish to cover their tracks, this can be done by hiding behind virtual private networks (VPNs) and concealing IP addresses. Perpetrators who know how to reboot routers can do this to erase their tracks, similarly, using IP addresses in households of multiple occupation means discerning the specific perpetrator is difficult:

> *I've seen cases where [perpetrators have] gone back and kind of rebooted the… hard drives… The routers and kind of got rid of any, put it back to kind of normal setting so no one would ever be able to go back and kind of find out that they've been on there.*

However, being open about the harassment was also indicated as being part of a more insidious intent to wield control over the victim:

> *In most instances they actually don't really try to cover their tracks ... they might make a fake profile, for example, for harassment, but they tend to want to, want the victim even to know who's contacting them.*

Perpetrators were described as making use of "inside knowledge" garnered because of their engagement with victims for a range of abusive purposes, including impersonation and hacking:

> *They know that if… they [the perpetrator] set up a Twitter account in their [victim's] mom's name and send them [victim] a message… they're going to accept it… They [perpetrator] have that knowledge of the individuals and so they're able to manipulate who they'll accept [as]… friends.*
>
> *… getting on to social media and manipulating it, changing photos, putting posts out as them [as the victim] and creating fake profiles in that person's name…*

In a more chilling example, a Helpline Responder detailed a case whereby the perpetrator had uploaded the victim's details on a message forum (e.g., Chan) for others (presumably strangers to both the victim and the perpetrator) to access and harass them too:

> *… she had loads of rude messages on Snapchat and loads of ads and she couldn't work out why… when she googled her Snapchat name. She found this Chan board which was full of the most disgusting and hideous comments about loads of different ladies and girls. Quite young girls and she found her name there with where she lived and a picture of her and it's kind of where the technology's now moved to.*

Perpetrators also carried out Image Based Sexual Abuse manipulation by using intimate photos or videos of victims to blackmail via "revenge porn" (i.e., to cause embarrassment or distress to victims by the release of intimate materials) or "sextortion" (i.e., to coerce victims to comply, stay, or do something by threatening to release intimate materials). Revenge porn and sextortion (sexual exploitation involving threats to release sexual images or information) usually involve the targeted release of materials to the wider public, or to specific individuals to maximise impact (e.g., professional or personal contacts):

> *… her ex-partner then was determined to just try and ruin her career… He had then... put the images out on the Internet and even… emailed her boss with these pictures… the ability to potentially get her fired from her job and ruin her life. It… basically it was revenge porn…*
>
> *… extortion... [is] common… They've got intimate photos or intimate information and they threaten to post online if they don't comply or whatever.*
>
> *I think revenge porn is more common in a subset of cases, for example where there has been a domestic abuse or coercive of control in a relationship. They tend to have that type of content and make those kind of threats. But I would say it was really aggressive in cases where there's high risk and quite aggressive threats or probably about… 20% of the cases.*

This section demonstrated the Helpline Responders' perceptions about TFIPV and the methods employed by perpetrators. They detailed recurring perpetration patterns, the simplicity of techniques, and how the COVID-19 pandemic impacted TFIPV perpetration. Figure 8 consolidates the themes discussed. The following section builds on this by presenting the findings related to obstacles preventing the effective response to TFIPV.

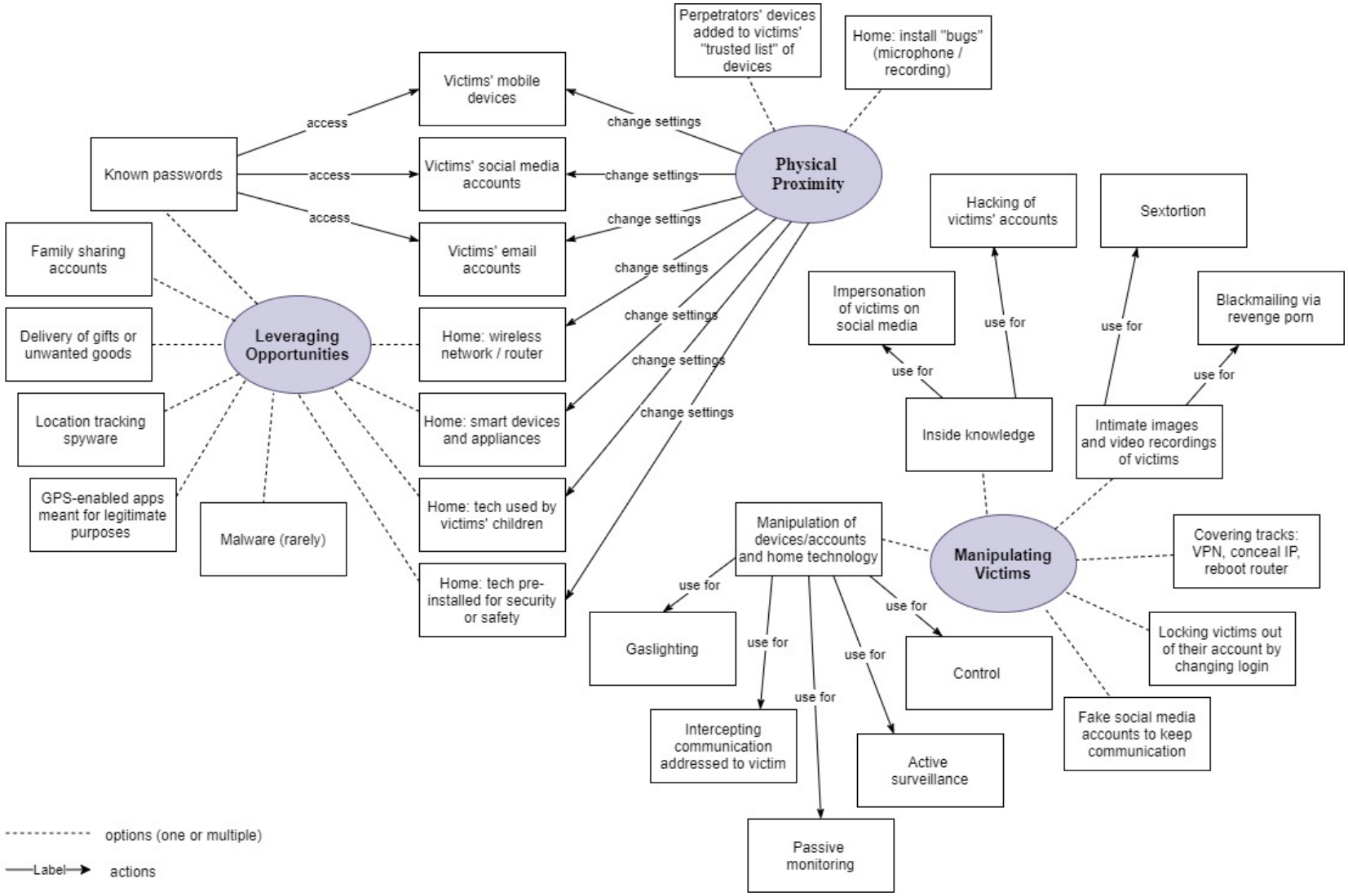


Figure 8: Consolidation of the 3 themes that emerged for technology methods used by TFIPV perpetrators.

Factors Impeding the Response to TFIPV

The fourth research question (RQ4) aimed to identify the factors impeding the countering of TFIPV. The findings have been grouped into three key themes: *victims' technological naivety, undue burdening* and *funding limitations***.** Importantly, the findings around funding resonated with, and underpinned, several other themes to emerge from this study.

Victims' Technological Naivety

The victim's lack of awareness regarding technological safety was a key area of concern and a significant impediment to ensuring effective responses. While knowledge disparities around cyber safeguarding were evident among those who had experienced TFIPV, most people were noted as failing to take suitable precautions due to not envisaging themselves becoming a victim of cybercrime:

> *People don't know about the risks and how to protect themselves until it actually happens to them*.
>
> *[Cyberstalking is] just so easy and it's less traceable, whereas you know if they turned up at their work there'd be so many witnesses of that and they would be, if they got questioned there'd be sort of like an alibi, where they were, whereas online it's just so much harder I think for the police to tackle it.*

Compared to physically following someone around, GPS tracking offers a very convenient way for perpetrators to covertly harass victims with very little effort. As noted above, the use of pre-installed software on devices that facilitates control and monitoring was one of the most common methods of TFIPV perpetration. Thus, victims being unaware of how these location services and programmes could be used against them was of concern to the Helpline Responders:

> *They don't realise that the find my function was there. They don't realise location and GPS were on their phone.*
>
> *Find my phone. It's really handy if somebody steals your phone... but it can also lead to somebody tracking you.*
>
> *They might have shared devices or they might have actually lived together, so it's a lot easier for them to have access.*

Perpetrators were noted to have often capitalised on this gap in victims' awareness regarding security measures, so this offered a useful starting point for the effective prevention of TFIPV:

> *Victims [need to be]... more aware of what is possible by people and kind of educate them in a way to secure things like their emails with two-factor [authentication]*

Due to the persistent and intrusive nature of TFIPV, victims' fears were often exacerbated by their lack of technological awareness, combined with the perpetrator's ability to instil fear

simply through threats of technological intrusion. As a result, victims develop a perception of being constantly at risk of TFIPV:

> *Yeah, another thing which is really, really common is... People get quite scared if their partners, or a lot of times they'll say that person that's harassing them is technical. Like, they have a friend who works in IT and from there they assume that they can do all this like crazy, elaborate, like, that kind of stuff you'd see in spy movie. Sort of when reality is a lot more simple than that and they're just scared of something, they don't understand.*

> *It's hard to distinguish what is... hyper-vigilance and what is actual symptoms of domestic abuse or cyberstalking, that type of stuff we see quite often.*

Helpline Responders noted that anti-virus software which can tackle programmes used to perpetrate TFIPV are currently available, yet victims are often unaware of this software, or fail to install it on mobile phones or tablets as most people only think to protect their computers:

> *An anti-virus that really focuses on the spyware and things that we see, would be really useful for victims.*

> *Like I said earlier, the antivirus are aware of spyware. If more people had anti viruses on their phones, less people would definitely be victims of this kind of... technology abuse because... the app wouldn't make it on there*

It was noted that it is easier for perpetrators to find information on how to commit TFIPV, than it is for victims to find helpful information online on how to deal with it:

> *… take the phone as an example, it's quite easy as soon as you have access quite easy. iPhones are more restricted in that in that regard, but with a bit of Googling it's easy for almost anybody to do it.*

> *I wouldn't say that even the perpetrator had that much knowledge it's just they knew where to look because of their motives. It was easier… if I would go now and put in Google, "how can I track a phone?" I would get 10 results. Whilst if I go and Google, "How can I stop the phone being tracked?" I might get 5.*

Undue Burdening

It is the victim's responsibility to gather evidence and prove that they are victims of TFIPV and/or stalking as part of their case. This puts the onus onto the victim to 'stop' the TFIPV whilst simultaneously allowing the perpetrator to continue, thus perpetuating victim blaming attitudes.

Victims are required to undertake inordinate amounts of work for their case to be processed. Yet, the Helpline Responders highlighted that their reporting does not always lead to an outcome, leaving victims feeling more frustrated. The Helpline Responders indicated the disappointment experienced by some victims who had reported their experiences of TFIPV to the police only to receive little help. Not only did they feel let down, but the experience had detrimental effects on their physical and psychological wellbeing:

> *Some cases you tell them to report to the police, they will tell you that I have done that, the police did not do anything. You know we have a lot of cases like that too. I think I mentioned one now before when somebody reported their case... so the police gave little or no help, so the abuse is going on and the person now is almost dying. So almost committing suicide.*

This, combined with the difficulty of evidence gathering and proving their own cases, perpetuates the potential for secondary victimisation, rendering victims unlikely to report their abuse:

> *They feel [the victim] like the buck stops at their reporting them [the perpetrator], and then nothing ever gets done.*
>
> *The evidence is so difficult in these cases because, you know, how do you prove that, you know, Bob, put this spyware on this woman's phone?*

The necessity of evidence gathering also makes it difficult for those helping them:

> *… trying to persuade someone [the victim] to not reset their passwords yet when you worked out that somebody is in there, you don't necessarily want to immediately alert that person [perpetrator]… you want to find everything out before you do it...*
>
> *… the key thing for me is getting that evidence gathering done so that we can take that to the police. Then from there, kind of, looking at securing devices when it's safe to do so. So, you don't want to secure stuff if it's still going to put them [the victim] at risk.*

The above issues highlight the gaps in processes and policies that hinder the countering of TFIPV. In parallel, Helpline Responders highlighted that these service response issues manifest due to a lack of police awareness and training in dealing with complex cases of TFIPV:

> *In terms of... the police especially it's, kind of, getting that training resource in and getting... some of the better police forces that are aware how to handle [TFIPV]*.

Emotional burdens were also noted as, unsurprisingly, most TFIPV cases involved an emotional/psychological element. This made countering TFIPV a more complex and arduous process for both the victim and the Helpline Responders (as non-IPV specialists):

> *I think, I think there's definitely a gap for like emotional support.*
>
> *When you get all the way through it and we've dealt with the technological side, [we're then] trying to find some way of supporting these people on an emotional level... which is nothing to do with us.*

The 'stay at home' directive also meant many victims were unable to seek help, particularly if they were living with the perpetrators:

> *A lot of people they live in... the house with their abuser and so it makes communicating with them almost impossible because they've [the perpetrator] got access to their emails. They're listening, they live with them. The only time they're getting [to] like contact you... is very rare and like very dangerous... That's effective in itself... from the perpetrator standpoint, because the victim's basically powerless because they can't get away from them. They can't contact anybody safely.*

Funding Limitations

Funding, and the lack of it, was a key area of concern among Helpline Responders, with many speaking about this in relation to the police specifically. To facilitate greater awareness of TFIPV, more funding for training was identified as a core factor in effectively dealing with cases and supporting victims:

> *From what I understand there is an issue with the police force being underfunded...*

Furthermore, participants noted the difficulty for small charities and organisations to obtain funding, even though these are the services that are most commonly supporting victims of TFIPV:

> *Another barrier is not just size of funding, it's also what funding is available for. So, if you're a domestic abuse charity, there's loads of domestic abuse funding. You know, if you're a kid education charity, there's loads of funds that say, "we're here to help kids' education". There are zero funds right now … to help victims of cyber-crime, and so you want to fund initiatives in that space.*

> *It's almost impossible because all the money goes... All the innovation budget goes to the big firms to innovate. You know Oxfam and [those] big charities. Actually, the small charities are going to solve the problem but can't get the money they need.*

Lastly, the lack of awareness and understanding of the complex nature of these TFIPV cases means that the funding and resources are not going to areas which may be key in countering TFIPV:

> *...There's little government funding in... in terms of knowledge for tech. I know they made a Christmas ad campaign with bits and bobs where... they're expecting kind of increases of tech over the Christmas period, but when you consider it now, that campaign's, kind of, gone down because nobody really remembers it ... Technology's meant to make your life easier, but it's also making people's lives easier for them to be trapped, to be hacked etc. So... I think funding is the biggest one in terms of that.*

This section of the analysis highlighted the factors impeding responses to TFIPV and how they can capitalise on victims' lack of technological expertise. It was noted that many of these issues arise due to a lack of awareness, combined with limitations in funding and resources. Leading on from this, the next section discusses the potential interventions to facilitate support for TFIPV.

Recommended Interventions to Tackle TFIPV

The final question (RQ5) sought to explore the Helpline Responders' recommendations for interventions to tackle TFIPV based on their professional knowledge and experiences. The findings have been grouped into five key themes: a heightened need to *focus on the perpetrator;* enlisting greater *stakeholder involvement;* embedding a *multi-agency approach* to support victims; a greater need for *educating the public;* and a need for *institutional changes* in criminal justice responses to TFIPV incidents and victims.

Perpetrator Accountability

Participants recognised that, alongside assistance for victims, interventions aimed at perpetrators were necessary to effectively recognise, respond to, and reduce TFIPV. Holding perpetrators to account was a core theme that emerged but Helpline Responders noted how difficult this could be to do in practice:

> *...it can be hard to detect the way that people are doing this, uh, stuff online, and even like, people with a bug in their house, in the physical bugging of ex-partners' houses, unless they find a device that's being used to listen to them, like, you'd never know...*

> *We can see that things are happening, but it's proving who's doing it. And for the police, even if the IP address that this unauthorised access is coming from is one that matches up to the suspect, they [the police] want to see the suspect physically doing that. So, for example, when they enter the house, that they've got that person's email up on the screen, because otherwise it could have been anyone in the household that's doing it. It doesn't necessarily mean it's that suspect.*

Alongside these impediments, Helpline Responders also hypothesised that some perpetrators were likely counting on the police's lack of specialist technological knowledge and inability or unwillingness to conduct thorough investigations:

> *I think, especially with like emails. It's such a hard thing to trace, and I think then that takes away the accountability from the perpetrator. So, I think if you could track these accounts more easily then there would be, sort of like, that threat for the perpetrator …*

> *… a lot of people do it because they can get away with it, because there's just usually no repercussions unless it can be proved ...beyond, like, unreasonable doubt or unless it becomes, uh, physical.*

Furthermore, it was noted by the Helpline Responders that, as well as loopholes in police awareness and practice, legislation regarding TFIPV is not stringent enough to enforce accountability on the perpetrator:

> *I think yeah, there just doesn't seem to be enough that the law, on the legal side of things, can enforce, like actually holding people accountable for the sorts of things that are doing online. There doesn't seem to be, I have never seen any case go far at all so, but that the effects it is having on the victim is still very severe.*

Helpline Responders suggested that not having adequate barriers in place to impede or investigate perpetrators was fuelling their ability to engage in TFIPV with relative impunity. Some had noted that perpetrators made efforts to cover their tracks:

> *I think they [perpetrators] do cover their tracks sometimes… clearing caches, clearing logins, that kind of stuff. But a lot of the platforms are now stopping that because the platforms don't let you clear your last logins for example… the way we tend to catch people out is when they make mistakes, which is when they, you know, read an email, click on an email and it becomes read before the other places. Read the email, or an email becomes unread, or a message vanishes or something … so yeah, I think they do tend to try and cover their tracks, but it tends to be much more about just by being quiet than it is by using actual technology to do that.*

> *… definitely make efforts to cover their tracks… having applications that seem benign but are actually malicious…you know, if they [perpetrators] created a login to something making sure it's not obvious that it's them, that type of thing.*

Helpline Responders recognised that perpetrators may become bolder and more insistent in their harassment because of their activities continuing and sometimes escalating without challenge:

> *… once somebody gets out of this relationship, that person might move onto another relationship. Now they will take the knowledge of what they did in the previous relationship to the next relationship. And sometimes, you know, they'll be able to jump a few steps in the monitoring techniques because they know how they were running in the previous one…*

Linked to this was the knowledge that perpetrators do not necessarily see their actions as wrong, or in other cases, feel justified in what they are doing (e.g., justified revenge for their partner ending the relationship). Helpline Responders therefore also recognised that without some form of perpetrator intervention the cycle of abusive behaviour was unlikely to end:

> *… You know they [perpetrators] are obsessed; their whole life is dominated by this individual [victim]… I think we do need to do more to help people spot that they might be in a cycle where it's unhealthy. You know these things can start with normal people having a bad break up. You still love someone… we have had instances in our cases where we have had people carrying out this abuse … approach us and say I think I'm stalking somebody. Or you know what? I, I just can't get out of it. What should I do? I do think there has to be something for these individuals to get help and understand what's happening…*

Stakeholder Involvement

Technology is a considerably profitable enterprise; hardware, software, mobile and online formats are popular, convenient and increasingly accessible. This can be argued to provide grounds for increasing expectations around social responsibility, especially from big companies, where they are profiting from both the use and abuse of their products. Social media organisations in particular were highlighted as a key stakeholder and relevant target for ensuring greater accountability to their service users:

> *Standards need to go out for software development and social media accounts about what should you do when you release a new social media platform. You know what security and protection you need to have in place. We need some standards that protect privacy and protect people who need help.*

Helpline Responders suggested that these companies could do more to block perpetrators, as they are often aware of what perpetrators are doing – and who they are – from the information provided by victims. Some (e.g., Instagram) were acknowledged to have implemented measures such as blocking new accounts from a previously barred email addresses, but others, Helpline Responders thought may need to be compelled into taking action. Similarly, Helpline Responders queried why verification measures such as the 'blue tick' symbol are not made more widely available to all users to prevent anonymous or false accounts:

> *I think the lack of a confirmed identity on social media platforms is one of the single biggest factors that enables the whole thing, and it's ludicrous really, because, you know, they have the technology to. You know, Twitter, all these platforms have a verified user scheme… you could verify your identity and get a little blue tick next to your profile.*

There were several similar recommendations for existing security measures to be made more widely available (or mandatory) to ensure greater online privacy and the protection of personal information. User verification and two-step authentication processes were strongly supported by many of the Helpline Responders, as these were seen as offering greater protection against TFIPV. However, these processes required more action from the organisational level to ensure this was embedded across social media platforms:

> *I think one thing that people have been campaigning for recently is that social media, or email accounts need ID before you log in or sign up. Whether that would be ethical in the slightest is one question.*
>
> *It wouldn't be changing the technology, but it would be enforcing the technology. So, things like two-factor authentication, which already exists, shouldn't be optional… And then there's a conversation to be had about can we make this better? Is there a way of simplifying it? Could it be done? But I think at the moment the technology exists to protect people better, it's just not being used.*
>
> *I think every email account should have two factor authentication on by default… Facebook and all the social media accounts having these things set up as default. Then have it, you know, complex passwords by default…*

Several participants had interacted with victims who sought help from social media companies following an experience of TFIPV. They critiqued the lack of consideration demonstrated and the considerable length of time it usually takes for victims to receive a response to their requests for assistance (e.g., removing fake accounts, abusive material or non-consensually shared images):

> *… the other kind of crazy thing with social media ... Some of these cases that, you know, the perpetrator is setting up 20 to 30 different profiles on Facebook to carry out the abuse, but they're all from the same computer – probably from the same IP address –*

> *and nothing is being done to say that's malicious activity. You could actually identify an individual. You could cut that out.*
>
> *Facebook and Instagram especially are ridiculously slow at getting these accounts taken down and they don't realize the seriousness and the impact it's having. So, I think just better responses from these companies*.

Similarly, the lack of interpersonal customer support available from social media companies was also cited as a particular source of frustration for both victims and the cyber specialists trying to advise them:

> *… there was no way that we could see that you could get in touch with human [support] at Facebook. You just have to go through. And it's not even like automated bots. It's like FAQ's [Frequently Asked Questions] … Well, none of these fit the situation. … You should be able to talk to a human.*
>
> *… take the ability for someone to flag a user of these platforms with the social media platforms or email companies, with any of the big technology companies is terrible and so trying to speak to somebody, trying to raise an issue trying to get someone to look at it is almost impossible… You need help when you need it. You need to block people. You need to show a video of you is on Facebook and you want to take it down. You need to be able to get to someone who can help you.*

Helpline Responders indicated that there was considerable scope for improvements in cooperation across different social media platforms. This is especially relevant considering multiple social networking sites are owned and operated by a single company. For example, Facebook also owns Whatsapp, Instagram and Messenger (which has the capacity to read and sync SMS messages into the app) among its 72 companies.

Similarly, Helpline Responders felt that organisations could do more to make it harder for perpetrators to install malicious apps or spyware on phones without victims' awareness or consent. Failing that, improved accessibility was recommended:

> *Having a single easy to use, sort of all-encompassing solution that someone could deploy to be able to be reassured that there's nothing malicious or untoward, so you know something that you could put on your computer, your laptop on your router, Wi-Fi network, and so have it deployed in an easy to use, non-technical fashion that you could say right? Yeah, I'm now locked down.*
>
> *Mobile devices with the minimum security settings enabled… Is a big problem*

However, Helpline Responders also noted that if people were confident and skilled enough to protect themselves online, there'd be less need for the products these companies sell therefore less of an incentive for them to reduce vulnerabilities.

Multi-Agency Approach to Victim Support

Victims who contact The Cyber Helpline during a crisis need to be dealt with in a way that does not worsen their situation. This can make imparting practical advice and support difficult due to having to do this remotely and with a victim who is potentially in a state of acute distress. For example, communicating with a victim via online means, such as via email,

requires caution if they are still living with the perpetrator, or if the perpetrator has access to their email accounts. This meant participants had to take additional care not to make the victim's situation worse or put them in further danger:

> *I think, as a charity, you don't want to say something that might potentially, like, poke the bear [antagonise the perpetrator]. ... you've got to have, like, their [the victim's] well-being in mind.*

Helpline Responders were therefore mindful of the implications around securing a victim's device when doing so could alert the perpetrator. Linked to this was the recognition that acting against a perpetrator (e.g., assisting the victim in blocking them on social media) may antagonise them and increase the risk to the victim. This led to the innovative use of approaches such as temporary mail to aid and support victims in a manner which foregrounded a safeguarding protocol. Helpline Responders noted that, in their experience, ex-partners often acted in a more aggressive manner online than comparable cases involving strangers. Therefore, they highlighted the importance of seeking professional help due to the potential offline harm that could arise following experiences of TFIPV:

> *… [making] direct threats, you know: 'I know where you are. I know you're going to be at this place at 5:00 o'clock'. Making threats tends to have a very, very big impact*.

However, Helpline Responders also acknowledged several important complexities related to assisting victims of TFIPV specifically, such as feelings of self-blame and reticence to involve the authorities. They recounted how some victims felt that they were to blame for what happened to them, which can impede their desire to seek out help and support:

> *… when they come to us there, there's an element of like being apologetic to us and not wanting to waste our time…*
>
> *Then there's a reluctance to call the police, but we would, in some of the cases, we would say that is serious enough to go and call the police even just to register it as a first step, so that in the event of any happening, you can say this is persistent. This is when it happened as a case number with the police…*
>
> *I think half the time when victims come to us, they're kind of lost because they haven't, first of all they're too scared to go to the police because they always feel like they've done something wrong when they haven't, and that the police don't always take them seriously or they don't understand what can be done.*

This illustrated the need for multi-agency working to ensure the specialist domestic abuse care victims may require was readily available, in addition to the practice support and advice provided by specialist organisations. Helpline Responders noted that there was scope for greater interaction between specialist technology organisations and dedicated domestic violence and abuse charities:

> *[In] any domestic violence case, like, the victim needs more support than just cyber support, and that's not something that The Cyber Helpline can really facilitate on their own. So, like, there's other charities which they work with … hand in hand.*

> *It's tough because, like, I feel there's, like, the cyber side of things, like, cyber security side of things. And then there's like the domestic violence side of things, and I feel, like, the, kind of, that point that you need two charities involved in those sorts of cases, like, we would cover the technical side of things and then an actual stalking charity would get involved to support the victim.*
>
> *Stalking charities are only half the picture. The Cyber Helpline helps that picture, but there needs to be further support to help anyone being stalked.*

Some participants felt unable to provide this kind of emotional support to victims (if focused on practical concerns) and expressed discomfort in dealing with victims of TFIPV without the adequate domestic abuse training. Nonetheless, some connectivity with other victim charities was outlined, along with signposting victims to specialist support.

Educating the Public

The Helpline Responders advocated a range of preventative approaches that focused on educating the individual and society about online safety, healthy relationships and online risks. Helpline Responders believed that victims generally lacked education or awareness about how spyware works, or how to check if they are being monitored, as well as how susceptible their software may be (e.g., the difference in accessibility between an Android and an IOS device). For victims with some inkling that they were under surveillance, many were still considered to be unlikely to know what to look for to determine if their device had been tampered with, or what to do if they find out it had been intercepted:

> *So, what victims sometimes don't understand when they have their Android phone is that there might be an application there with an icon which looks like an app which they usually use, but actually hidden behind that app is actually spyware which is potentially reading their messages, sharing their location, being used as a … recording device. And I think that that's the hardest thing to detect ... kind of working out on a mobile phone: Is there something that is opening up their life to a perpetrator which they're just unaware of?*

Some Helpline Responders recognised that perpetrators will be aware that the victim has multiple apps on their phone and thus will not notice additional ones added covertly or which do not raise suspicion:

> *A big thing is, uh, people have so many apps on their phone, like, so many apps on their phone that they don't know… I've had cases where people have had, like, well over 100 apps on their phone… and I've asked them to do, like, an app review and, like, remove the ones that aren't necessarily.*

Helpline Responders also recognised that cybersecurity is a complex issue beyond many people's understanding, which can make advising the public difficult. Some indicated that they themselves were unsure of how some social media prevention mechanisms operate, demonstrating that even experts can be confounded by things members of the public are meant to comprehend:

> *If I'm looking at my Google account or my Gmail address and I'm trying to find who, like, what the last login attempts where for my code, it could be quite difficult for me to find it and I work in cybersecurity.*

Several Helpline Responders therefore recommended the implementation of accessible and comprehensive tools for victims for enhanced personal safeguarding to become standardised online behaviour.

Highlighting the range of methods and tactics used by perpetrators may offer effective insight for personal safeguarding. Increasing victims' online safety involves making them aware of the ways in which perpetrators may gain access to their accounts, covertly or otherwise. For example, perpetrators may use pre-collected digital content at a later point, therefore people need to be wary about sending such content or making this available somewhere it could be accessed by a perpetrator. Similarly, perpetrators may offer phones as gifts, or offer to install programmes on a victim's phone, as a pretext for loading them with spyware:

> *So, ... the attacker was ... quite knowledgeable and the victim was obviously, kind of, surrendering their device, and at that point you didn't know what was on there, because quite often they had, like, stalking software where you can just, kind of, see what's happening on the phone and ping it and see where it is.*

This linked to wider messages about not allowing someone physical access to a phone in case they used this opportunity to install spyware or check messages. Relatedly, while sharing passwords for accounts such as Netflix may seem innocuous at the time, people need to be aware that this may render them vulnerable later if perpetrators are aware that these passwords are similar to others that the victim used elsewhere.

This all implied a greater focus on healthy relationship advice, so potential victims were alert to behaviours which could indicate concerning conduct:

> *Have a relationship with someone they think it's, you know, it's normal for someone to be going through their phone and all their emails and stuff, and they'll realize that's not necessarily something that actually … that's perhaps quite controlling.*

> *We need … [to] educate people about what a healthy relationship is, which is key to domestic abuse [prevention], we need to educate people about what's normal at the end of a healthy relationship or in the relationship.*

On a societal level, Helpline Responders suggested that the mainstream media could do more to highlight the varied nature and impact of TFIPV. This may be especially important in breaking down stereotypes (e.g., phishing emails; sharing passwords as a behavioural trait affiliated to younger people) in order to show increasing sophistication around perpetration, or hidden vulnerabilities of potential victims. This may also prove important for challenging victim-blaming attitudes and lessen victims' feelings of culpability, as noted by some participants.

Institutional Changes

All the participants stated that significant improvements could be made to the current criminal justice response to TFIPV and those victimised in this manner. Several recognised the

limited understanding and application of existing legislation by criminal justice actors to protect victims or prosecute perpetrators, while others suggested that a revision of these laws and policies was necessary. Some participants suggested that police and prosecutors currently underuse available legislation, such as the Computer Misuse Act or Malicious Communications Act, while others suggested that existing legislation needs to be strengthened to enhance protections and punishments:

> *So, the guidance, the policy, the regulation, legislation in place. It's just not being followed as much as it could be ... The police aren't trained on it, and the general public aren't aware of it.*

> *… better defined guidelines and legislation for this crime. It needs updating for sure, like all those Computer Misuse Acts that, like, they're way outdated for, sort of, the modern age.*

There was a sense that most victims lacked awareness of existing (victim-focused) legislative protections, and thus may be less likely to benefit from enhanced criminal justice measures unless these were made widely known:

> *So, for example, stalking Protection Orders quite a new thing that's accessible, which is - I guess it's put simply a restraining order for victims of stalking… But we don't see them being used, and even when, kind of, I've spoken to victims and asked has anybody told you about this that they have no idea what that means.*

Interestingly, one Helpline Responder recognised that taking a victim-focused approach to address this issue may prove counterintuitive as it could create behavioural thresholds, hierarchies and typologies which leave victims reticent to report abuse or seek help. To be more relatable, and address a wider pool of potential victims, they suggested that it would be better to focus on the perpetrator and their activities instead, not the impact on the victim, when tackling this issue.

Recognising that most victims interacted with the police in the first instance, there was a shared sentiment among participants that the police could do more to help victims who report TFIPV. Several participants noted considerable variability across different police forces in terms of officers' responses and levels of specialist knowledge, and willingness or ability to help victims:

> *… it's kind of a postcode lottery in terms of how the police will deal with you. You know, there are some police forces like West Yorkshire and Kent Police who are just experts at what they do and anytime I've had a victim that has dealt with them they've just been amazing. But then there are other police forces … and they just didn't really know.*

> *I know some of my victims actually contacted the police… And a couple of times didn't even get a reply back.*

Several Helpline Responders indicated their frustration at the repeated deployment of inexperienced officers, often new to policing, in cases involving TFIPV:

> *… that tends to be what we see happen … junior officers often are kind of given these cases… … I don't think the police are trained on that at all, especially when they are sending junior officers out. They haven't had that cyber crime training.*

Furthermore, deploying low ranking and inexperienced officers to cases, usually with no prior cyber training as indicated, often had negative implications for victims' cases. For example, some police officers had advised victims to do factory reset of their phones, wiping evidence of the abuse in the process:

> *… in terms of gathering evidence, the CPS guidance is not to wipe the phones ... But what we tend to actually see is that as soon as they [victims] go to the police, the police are saying to them 'oh just do a factory reset, get rid of the phone, get a new one'… And straight away, that's getting rid of so much evidence.*

Not only is this counter-intuitive for prosecutorial purposes, but such advice may also damage victims' access to justice if the abuse escalates.

A more pressing issue was Helpline Responders' perceptions from victims that some police officers were reticent to investigate cases (e.g., by not collecting evidence), or appeared only to do so at a point where the situation had escalated to a more serious level (e.g., the perpetrator had threatened to harm the victim). Helpline Responders expressed frustration with the some of the approaches police were seen to take:

> *a lot of time people would come and they would say that the police aren't helping ... It can be really, really hard for the police to connect on that sort of stuff, because they just, maybe they don't have the, sort of, right teams to investigate that sort of stuff.*

> *Well, again a lot of time, like the police just don't have the knowledge and they don't have time to investigate that sort of stuff. … they [victims] would say: well, we've contacted the police and the police have done nothing or the police say it is not enough evidence, but there's not really, like, a defined like amount of evidence*

> *Like a lot of people were worried that, yeah, they were stalked and that, but nothing was going to happen until they were attacked and like, that's like was just horrible to think about, like where a lot of people feel like folk can just do whatever they want to them online and the police aren't going to do anything until they're physically harmed*

> *police forces [need] to understand when a victim comes to you, you need to see that you need their technology. You need their devices. You need to, kind of, you know, take a copy and need to take it seriously. A lot of them will just say: 'Go and run an antivirus and the antivirus will find anything, you're fine' ... maybe the CPS don't see it as a big win and find it too hard to prove that the perpetrator's doing it.*

Other critiques included failing to respond effectively to victims beyond providing a case reference number, failing to adequately safeguard victims following a report (e.g., bug sweeping) and not informing victims of investigative processes:

> *a lot of time the police will take their [victims] devices, but then then what are they doing with them? Like we don't know? There's not really visibility on that either.*

Helpline Responders provided several reasons as to why the police may be reticent to take online abuse seriously. These included a general lack of understanding around the nature of the abuse, and what a suitable amount of evidence looked like to investigate a report. This meant that the police were often reliant on technology organisations for their specialist advice and input on cases, and that charities such as The Cyber Helpline often ended up acting as a conduit between the victim and the police, which was considered acceptable up to a point:

> *You shouldn't really need to have to get in additional charities to help you gather evidence on all your devices to then take that to the police. Like surely the police should have that kind of capability and functionality themselves to help victims with that.*

> *I think that what we really need is a justice system that is brought up to date with how technology works.*

Helpline Responders highlighted the need for an improvement in the consolidation of information (e.g., police reports, applications for specialist assistance) to build a more comprehensive picture of what is happening to the person over a period, what help they might need and what the CJS can do in response:

> *Let's report all online problems in one place where we can actually look at this and say this is one user who has reported 50 incidents in a month. Maybe it's not a bunch of separate things. Maybe this is a wider campaign of stalking or abuse, or harassment, and we need to pull all these data points together. So, I think kind of the user experience of reporting, and having that single view of the victim [is needed].*

This lack of a joined-up approach was coupled with the recognition that such technologies may be inaccessible due to the high costs involved:

> *I'm sure like the technology is out there, it's just expensive. So, then charities can't use it. And then that probably, like, affects their ability to get evidence and take it further with the police so I think the technology definitely exists. It's just not available … for the companies that probably need it the most.*

Suggestions also indicated a greater need for international co-operation between justice systems and co-ordinated responses between domestic violence police networks, along with police forcing companies to share information related to harms and abuse.

Part 3: Online Survey

This section presents the findings from the online survey. It should be noted that, whereas the term TFIPV has been used throughout this report, the online survey used the original definition of technology facilitated domestic abuse (TFDA) therefore appears as such in the below diagrams.

Participants' Experience

According to the responses by 16 volunteers, the minimum amount of volunteering experience at The Cyber Helpline was two months. The longest period of volunteering at the

charity was 48 months, which was since the helpline was founded. Participants' overall experience of working with individuals who have been victims of cybercrime also ranged from 2 to 96 months. Figure 9 shows the average experience at The Cyber Helpline and the average overall experience working with individual victims of cybercrime. The average volunteering experience at The Cyber Helpline was a little over 15.5 months and the average overall experience of the participants with victims of cybercrime was over 17 months.

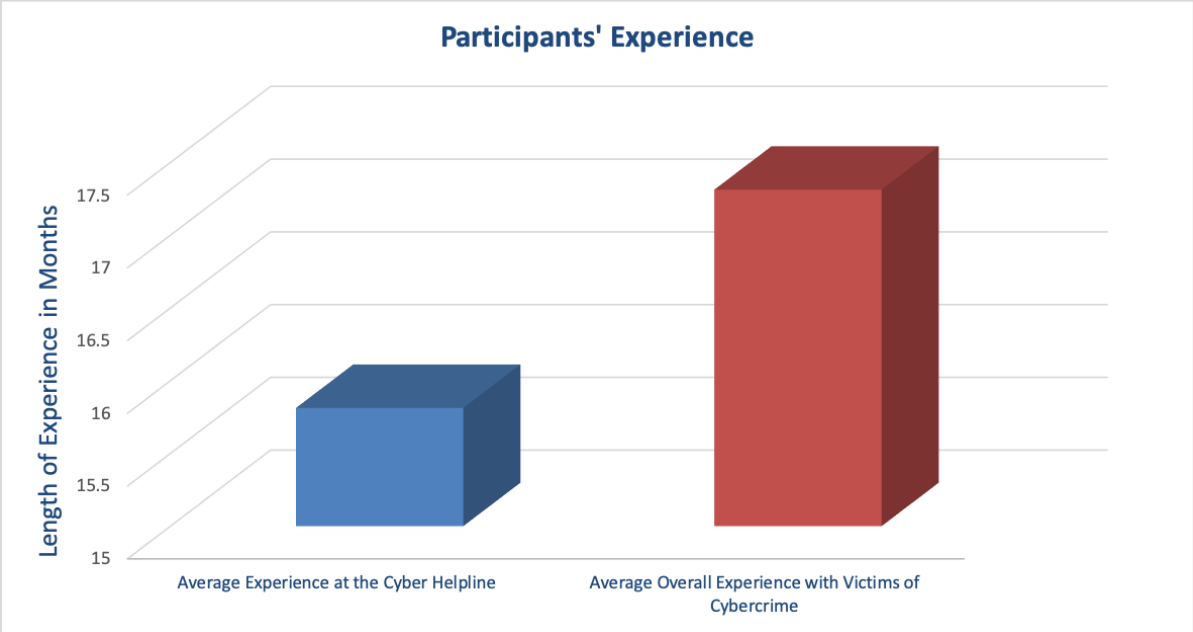


Figure 9: Participants' average length of experience at The Cyber Helpline and average overall length of experience of working with victims of cybercrime.

Victims' Digital Vulnerabilities

The participants' ratings for the frequency of victims' digital vulnerabilities, overall, shows a varied level of agreement on the frequency of each statement, as shown in Figure 10.

For almost all statements representing a digital susceptibility of victims, participants reported a varied level of frequency. Despite the wide range of reported frequency for the victim vulnerabilities in general, the ones which reached strongest agreement among participants including *often* and *always* were:

- "use of shared passwords with the perpetrator" (63%),
- "use of the same password for several accounts and online services" (69%),
- "use of weak privacy settings for social media accounts" (75%), and
- "no use of multi-factor authentication for access to devices and/or apps" (76%).

The strongest disagreements including *never* and *rarely* were: "use of jailbroken phone" (62%), and "use of phone with non-default location-sharing apps installed (e.g., spyware or apps designed for parents to track kids)" (50%) – although 31% indicated it *sometimes* happens.

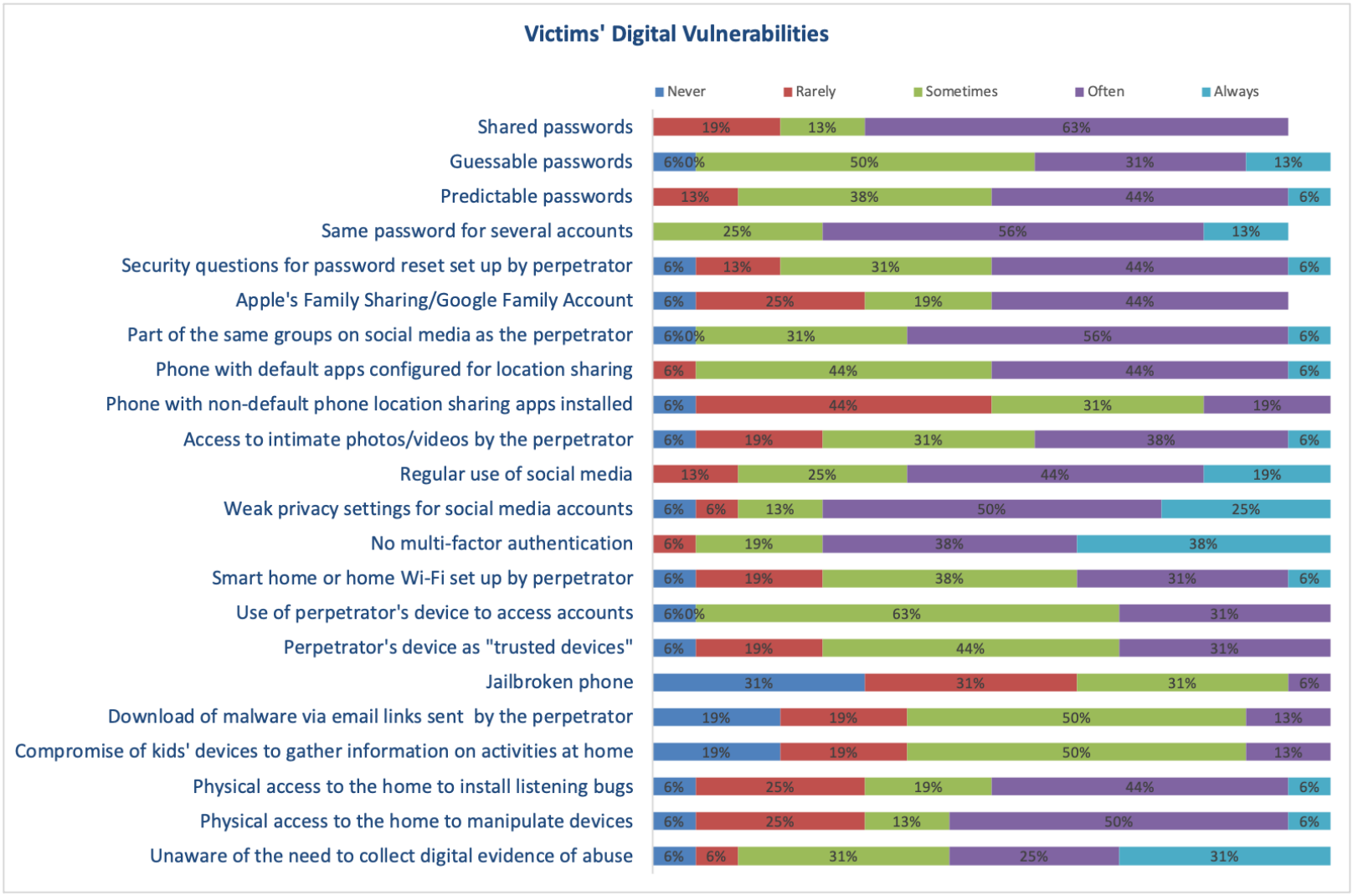


Figure 10: Participants' ratings for the frequency of victims' digital vulnerabilities.

Gaps in Countering TFIPV

Technology Related Gaps in Countering TFIPV

The technology-related gaps in countering TFIPV are shown in Figure 11. The results show that all participants either *strongly agreed* or *somewhat agreed* that victims are unable or unaware of how to audit who has been connecting to their home Wi-Fi network as well as who has been accessing their accounts or devices, such as their email, social media, smart home devices, or phone. In addition to these, all participants either *strongly agreed* or *somewhat agreed* that it is difficult for victims to understand the extent and consequences of privacy settings of online platforms.

Although none of the participants strongly disagreed with any of the presented statements of technology related gaps in countering TFIPV, the statement that received the most varied level of agreement by the participants was the lack of available features to enable people to lockdown their accounts on specific devices.

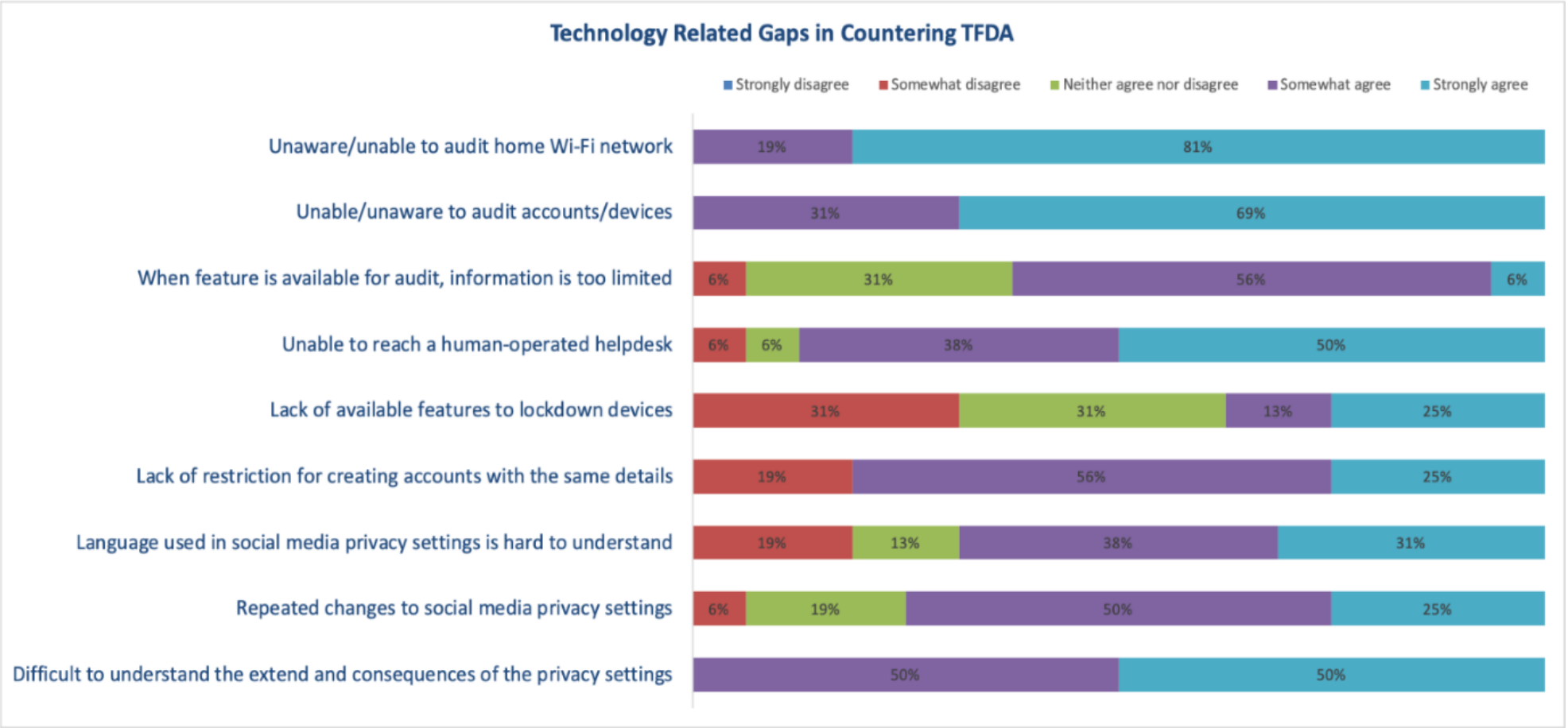


Figure 11: Participants' level of agreement with the technology related gaps in countering TFIPV.

Non-Technology Related Gaps in Countering TFIPV

Participants' level of agreement with the non-technology related gaps in countering TFIPV, overall, showed a similar pattern. As shown in Figure 12, most participants either strongly agreed or somewhat agreed with most of the non-technology related gaps, which shows that each of these statements indicated a non-technology related gap in countering TFIP.

According to the participants' responses, the three most prominent non-technology related gaps were that TFIPV can manifest in a range of different ways, there is a lack of funding to help victims of cybercrime in the UK, and that charities play an important role in supporting victims of TFIPV. The participants' strong and consistent agreement on these statements suggest a consensus that TFIPV can manifest in a range of different ways, such as in physical, digital, and online or cyber forms. Similarly, the participants' strong and consistent agreement support that lack of funding, such as government funding, to help victims of cybercrime in the UK is a non-technology related gap in countering TFIPV. In addition to these, more than 90% of participants agreed that charities helping victims of cybercrime perform an important role in supporting TFIPV victims.

The only statement in relation to the non-technology related gaps in countering TFIPV which received a more varied level of agreement by the participants was the partnership between existing cybercrime services and other front-line responders, including the Police and the NHS. The findings suggest that 32% of the participants either *strongly disagreed* or *somewhat disagreed* with the presence of good partnership between cybercrime services and other front-line responders.

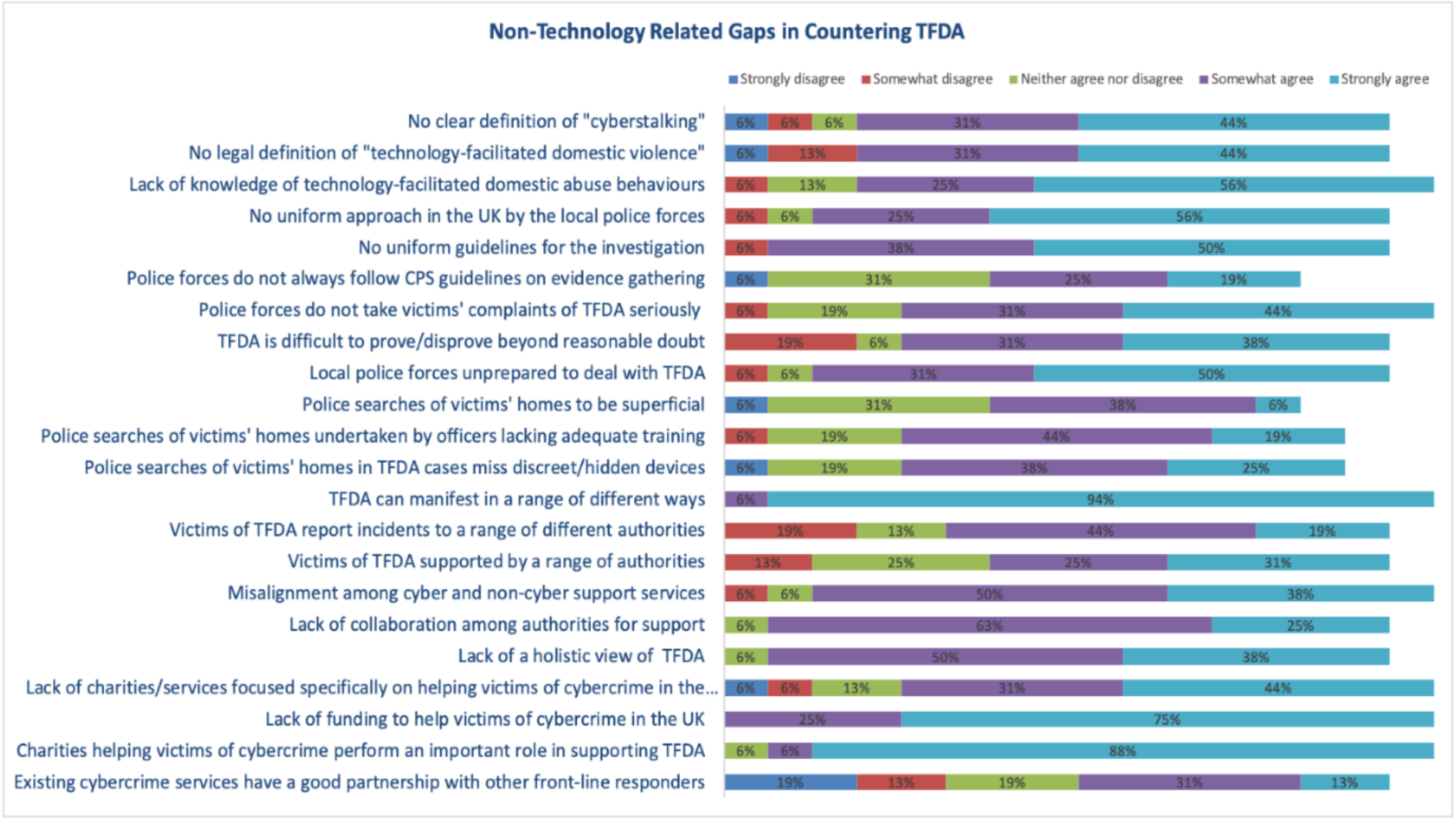


Figure 12: Participants' level of agreement with the non-technology related gaps in countering TFIPV.

Recommended Interventions to Address TFIPV

Participants' responses to the recommended interventions to address TFIPV, overall, showed a similar pattern in their agreement levels. Figure 13 shows the participants' level of agreement with the proposed recommended interventions to address TFIPV. Findings suggested that most participants strongly agreed with almost all recommended interventions needed to tackle TFIPV.

The two recommended interventions, "social media platforms should automatically block accounts created using the same email, phone number or that originated from the same IP address as a previously blocked account" and "automatic alerts should be issued to individuals when reaching a threshold of downloads and/or online purchases of material relevant for perpetrators of TFDA" were more controversial and received less agreement compared to the rest of the recommendations. However, more than 60% of participants still either *strongly agreed* or *somewhat agreed* with these two recommendations.

More importantly, all participants either *somewhat agreed* or *strongly agreed* with the following four recommended interventions to tackle TFIPV:

- (online) accounts should have safe settings enforced by default (e.g., multi-factor authentication);
- legislation should be updated to recognise different types of cyber-related and/or technology-facilitated crimes, such as "cyberstalking" and "TFDA";
- local police forces across the UK should provide training for first responders of TFDA; and
- local police forces across the UK should standardise and improve their response to suspected TFDA.

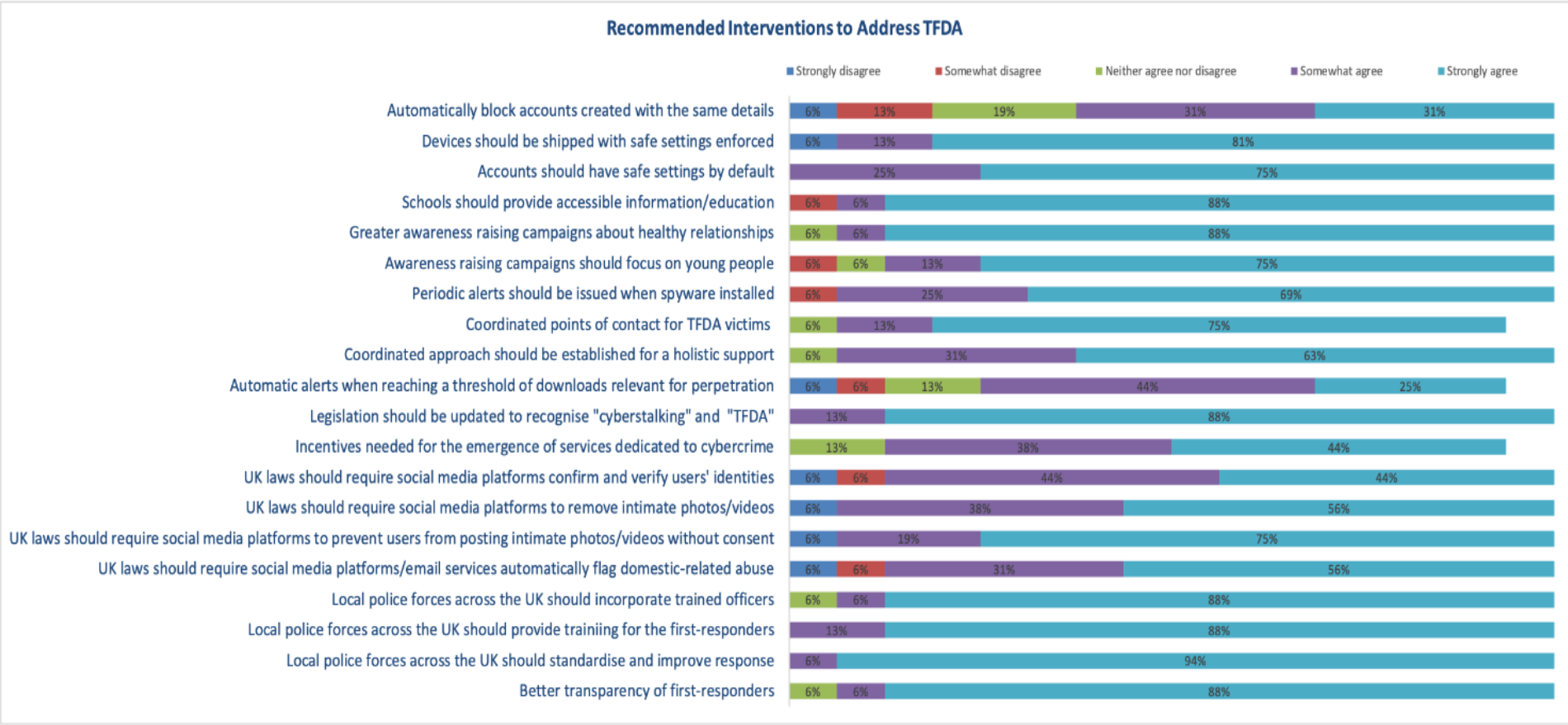


Figure 13: Participants' level of agreement with the proposed recommended interventions to address TFIPV.

Despite the fact that trustworthy conclusions cannot be drawn from the online survey, as elaborated in the methodology section, the survey participants indicated a consensus that helps focus proposed interventions for TFIPV, complementing findings from the interviews. For example, sharing of password between victims and perpetrators in the context of an intimate partner relationship seems natural. However, education about risks to the public (a theme that emerged from the interviews) – specifically tailored to the scenario of when a "relationship goes wrong" – could resonate better to potential victims and make a bigger impact to reduce this digital vulnerability in the context of TFIPV.

Another interesting finding from the survey was the strong consensus that weak privacy settings is a common vulnerability among victims, and this can be linked with the strong agreement that victims find it difficult to understand and judge the impact of privacy settings.

The recommendations that ranked higher in terms of agreement among the survey responders covered technology, (e.g., safe settings enforced by default), legislation (e.g., recognition of cyber-related and/or technology-facilitated crimes such as TFIPV), and Police response to victims of TFIPV, again give a sense of priority for findings from the interviews.

Discussion

Our research obtained valuable insights from The Cyber Helpline Responders, drawing on their experiences of dealing with victims of TFIPV. Our findings have contributed to this developing area of analysis by indicating the myriad ways in which perpetrators utilise available technological and online methods to victimise their targets.

Emergent themes regarding methods of TFIPV indicated that perpetrators leverage the types of technology that is often part of victims' daily lives, such as mobile phones, social media accounts, and smart devices. Others involved taking advantage of the trust built with the victim during their intimate relationship. This meant perpetrators did not necessarily require or employ advanced technological skills to abuse.

Many of the techniques used by perpetrators relied on having physical access to the victim's (or their children's) devices or home environment. A growing number of homes feature smart (Wi-Fi-enabled) devices and applications with the capability of communicating with each other and being controlled remotely. Perpetrators tend to oversee the creation and configuration of accounts, personal devices, Wi-Fi routers, surveillance systems and smart devices around the house for victims. This access can later be used to enable abusive behaviours through the direct manipulation of technology and psychological manipulation of victims via this technology.

The Helpline Responders considered that the onset of the COVID-19 restrictions provided an opportunity for perpetrators to improve or acquire new skills relevant for TFIPV, or even to consider TFIPV in the first place. An increase in the number of TFIPV cases, and in the intensity of abuse (which became more cyber-dependent), was also noted during the "stay at home" directives informing national lockdowns. Victims felt increasingly trapped since the option of going offline to escape abuse was no longer feasible, while perpetrators resorted to creative methods of TFIPV through the delivery of gifts and unwanted items to victims. As research

continues to emerge on this issue, our findings provide a necessary basis from which to examine TFIPV in the COVID-19 climate.

A range of factors were identified as negatively affecting the ability to counter TFIPV. The accessibility of technology and availability of 'how-to' information provides perpetrators with opportunities to engage in a range of TFIPV behaviours relatively easily. The anonymity provided by the online space and the ability to operate covertly lessens the ability to hold perpetrators to account.

Reducing the ability to perpetrate TFIPV and improving the support available to victims requires greater investment by social media and technology companies. Presently, victims can face considerable difficulties when trying to engage with social media companies as part of their efforts to have action taken against perpetrators. There is scope for these companies to leverage existing technology by emphasising security-by-default to help victims protect themselves better online.

Members of the public are becoming increasingly familiar with two-step authentication processes as they are regularly embedded in high-stakes accounts (e.g., online banking, work VPN etc). Rolling these out more widely means they would become normalised, therefore enhancing security across a range of personal accounts. However, social media companies who impose these measures without adequate information, or who continually update privacy settings without warning, can render victims vulnerable if they are unaware of how to implement these enhanced measures, or what kinds of information remains accessible on their social media pages following privacy changes.

Experiencing TFIPV can have significant impacts on victims and impede effective responses if victims do not realise what is happening, feel reluctant to address what is happening, or are isolated with the perpetrator or away from support networks (e.g., friends and family). Limiting their online habits can lessen the likelihood of victims seeking specialist help and advice from online sources.

Participants cited awareness of the frustration some victims experienced upon reporting abuse to the police when cases were not followed up, or where officers were unfamiliar with how to address TFIPV. A lack of funding also emerged as an overarching issue and one that underpins the ability of a range of services to provide a more holistic support to victims. This could be aligned with accessible education campaigns about online safety, healthy relationships and awareness of susceptibility to online risks and harms.

Workstream 4: TFIVP Infographic, Project Conclusions and Recommendations, Tackling TFIPV Toolkit

The final section (led by CoI Duggan in consultation with the research team) provides a consolidated overview of the collective workstream findings. It is divided into three parts:

TFIPV Infographic

We worked with a professional design agency to produce an image that provides a clear overview of our project findings and recommendations.

Project Conclusions and Recommendations

We provide a thematically organised, narrative overview of our findings and what they mean, alongside suggested measures for implementation. We highlight gaps in knowledge and outline recommendations for policy, practice and the public, alongside suggested amendments to current legislation. Furthermore, we draw from our multidisciplinary perspective to identify areas for further research.

Tackling TFIPV Toolkit

We provide an accessible list of suggestions for actions that can help various stakeholders recognise, respond to, and reduce TFIPV perpetration. These are accompanied by images indicating the relationship between the various situations, stakeholders and suggestions outlined.

TFIPV Infographic

The infographic below details our findings in a clear and accessible manner, along with a "toolkit" offering advice to help recognise, respond to and reduce TFIPV perpetration.

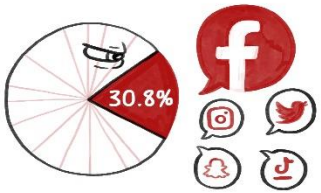
WHAT WE DID...

THE HOME OFFICE FUNDED RESEARCHERS AT THE UNIVERSITY OF KENT TO INVESTIGATE THE PERPETRATION OF TECHNOLOGY FACILITATED INTIMATE PARTNER VIOLENCE (TFIPV)

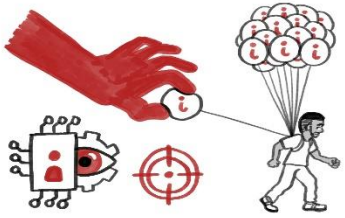
OUR RESEARCH INVOLVED PARTNERING WITH THE CYBER HELPLINE TO EXPLORE TFIPV USING THEIR ANONYMISED CASE FILES. WE ALSO CONDUCTED INTERVIEWS AND A SURVEY WITH THEIR HELPLINE RESPONDERS

EXTORTION WAS MORE COMMON IN BRIEF RELATIONSHIPS OF A FEW MONTHS OR LESS

WHILE UNWANTED CONTACT AND COMMUNICATION AND UNAUTHORISED ACCESS WERE MORE COMMON IN LONGER TERM RELATIONSHIPS



ALMOST A THIRD OF REPORTED TFIPV CASES INVOLVED SOCIAL MEDIA, WITH FACEBOOK THE MOST FREQUENTLY USED PLATFORM



PRE COVID, TFIPV PERPETRATORS FREQUENTLY UTILISED MORE COMPLEX TECHNOLOGIES TO SURVEIL TARGETS AND OBTAIN PRIVATE INFORMATION

DURING COVID, TFIPV PERPETRATORS MORE OFTEN UTILISED AVAILABLE ONLINE INFORMATION E.G., FROM SOCIAL MEDIA, OR RECORDING VIDEO CALLS TO COMMIT EXTORTION

WHAT WE FOUND...

TFIPV INCREASED DURING COVID-19

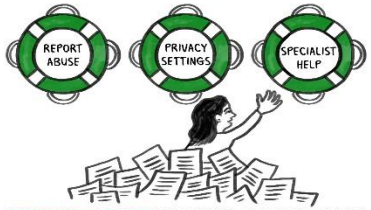
THE CYBER HELPLINE SAW A 420% INCREASE IN REPORTED CASES

TFIPV CAN BE GROUPED INTO 5 CATEGORIES

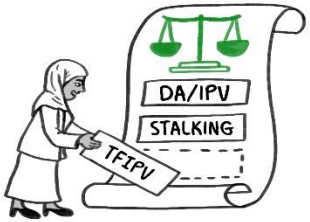
TFIPV PERPETRATORS ACCESSED ACCOUNTS AND SMART DEVICES VIA EASILY GUESSED OR KNOWN PASSWORDS

SHARED SPACES OR PHYSICAL PROXIMITY TO VICTIMS ALLOWS TFIPV PERPETRATORS TO MANIPULATE DEVICES, CREATE FAKE ACCOUNTS, INSTALL BUGS AND TRACK LOCATIONS

WHAT WE RECOMMEND...



SPECIALIST SUPPORT FOR VICTIMS IS AVAILABLE, BUT SYNERGY BETWEEN SAFEGUARDING AGENCIES AND CONSISTENT FUNDING IS NEEDED. TECH COMPANIES AND SOCIAL NETWORKING PLATFORMS NEED TO MAKE IT EASIER TO IDENTIFY AND SANCTION TFIPV PERPETRATORS



TFIPV IS A SERIOUS FORM OF ABUSE. IT SHOULD BE CONSIDERED AS PART OF THE UMBRELLA OF DOMESTIC VIOLENCE AND ADEQUATELY REPRESENTED IN LEGISLATION

FOR HELP AND SUPPORT FOR TFIPV VISIT - WWW.THECYBERHELPLINE.COM

University of Kent | Institute of Cyber Security for Society (iCSS)

Project Conclusions and Recommendations

Defining TFIPV

The multiple terms used to describe the range of behaviours comprising TFIPV makes it difficult to provide an overview or comprehensive picture of this offence. The existing literature offers a wide range of descriptors for TFIPV, with these descriptors often changing over time and in response to the growing awareness of the different TFIPV behaviours implicated. While TFIPV can be considered an umbrella term for a wide range of abusive actions, it is important to recognise its dynamic nature, and the difficulties which may be encountered in trying to categorise, quantify or measure such a rapidly evolving offence. Similarly, there may be multiple factors informing different interpretations of what constitutes un/acceptable conduct online and in relationships. This means that both victims and perpetrators (and, more widely, members of the public, practitioners and policy makers) may harbour different perspectives of, or hold different thresholds for, what constitutes TFIPV. Our findings also indicated that it is unhelpful to consider online and offline forms of abuse and harassment as separate or unrelated. In some cases, there may be an overlap or a progression from one form of abuse to the other. Where both are being experienced, there is a danger that people (e.g., victims, criminal justice agents or practitioners) may – consciously or otherwise – impose a hierarchy of the behaviours based on perceived risk of harm and victim impact.

Recommendations:

- **The terminology, definitions and behaviours comprising TFIPV should be harmonised and agreed upon. This will result in more accurate prevalence and co-morbidity rates.**
- **TFIPV should be adopted as the recognised term comprising of the full range of behaviours and actions associated with it and possible permutations.**
- **The legal definition should be broad and sufficiently flexible to incorporate the changing nature of technology and subsequent changes to TFIPV.**
- **TFIPV should be recognised to inform part of wider IPV behaviours and considered equally as serious and impactful for victims.**

TFIPV Victim Profiles

The perpetration of TFIPV cuts across all generations and profiles, although our review indicated that the available academic research has predominantly focused on younger, female victims. The general profile of TFIPV victims has also been heavily informed by quantitative studies which targeted populations aged from early adolescence to mid-thirties

and were disseminated via educational establishments (e.g., schools, colleges and universities). Many studies, which had a larger female samples or were solely focused on female participants' experiences, reflect the gendered nature of IPV, alongside incidence and prevalence rates for female victims routinely being higher than for males. Similarly, our research findings indicated that most victims were female, and the perpetrators were male (albeit of undefined ages, but primarily adults).

Our review suggested that studies which indicate gender parity in terms of perpetration should be treated with caution as they fail to account for contextual factors such as impact or intent. In these studies, female participants reported engaging in more covert and less serious forms of TFIPV (such as monitoring a partner's social media or phone) whereas male participants reported engaging in more overt and severe TFIPV (e.g., antisocial, predatory, and IBSA behaviours).

Recommendations:

- **Further research is needed which focuses on a wider victim and perpetrator demographic to provide more representative insight into TFIPV experiences and online habits.**
- **TFIPV needs to be examined by including a wide range of relationship types to verify the differences found in this project (e.g., short-term relationships linked to extortion vs long term relationships linked to unwanted contact and communication and unauthorised access) and identify further differences that may assist with prevention and case management.**
- **A greater commitment to qualitative and longitudinal research is required to explore patterns and trends in TFIPV over time.**
- **Much more research with TFIPV perpetrators is needed to establish motivations and risk factors for TFIVP, and to tailor prevention and interventions accordingly.**

Recognising TFIPV and Tailoring Safeguarding Advice

Victims may have different thresholds for what they consider to be abusive conduct which can influence whether and when they disclose their victimisation. Studies indicated that gender may be an explanatory factor in disclosure; female participants in the studies reviewed were more likely to readily acknowledge and disclose *offline* abusive behaviours but required prompting to impart information about being victimised online. By comparison, male participants were more forthcoming about being subjected to online monitoring and surveillance behaviours. Gendered notions of surveillance (e.g., this being normalised for women but not for men) may mean that male victims of TFIPV acknowledge abuse more readily.

Our research found that many male perpetrators reportedly began engaging in TFIPV following the breakdown of a romantic relationship. In these cases, perpetrators were shown to be motivated by jealousy or hostility towards the victim. Perpetrators were able to leverage their intimate knowledge and interactions with victims to commit TFIPV. They used social

media as a resource for monitoring, controlling and abusing victims online. Sometimes, they surreptitiously accessed the victim's private social media or email accounts, either to surveil the victim or to interfere with their private communications. The breaking down of a romantic relationship can potentially blur the boundaries of what is an acceptable form of surveillance, especially with respect to social media accounts. Perpetrators who feel justified in checking up on victims or harassing them online (rather than in person), may feel less compelled to desist if they consider their actions to be reasonable.

Our research also indicated the importance of discerning between different age profiles to better understand the nature and impact of TFIPV and tailor relevant information and support appropriately. Victims contacting The Cyber Helpline for assistance tended to be older than the general profile of TFIPV victims as identified in the academic literature. Generational profiles are important to identify due to differences in types of TFIPV experienced, the impact on the victim, and their willingness or ability to seek help. Furthermore, age may prove relevant when considering the medium through which to disseminate preventative and safeguarding advice. People aged 30 and older prefer using platforms such as Facebook and communication methods such as email, whereas younger adults are showing preference for Tik Tok or Instagram and communicating via direct or instant messaging.

The differences in the types of TFIPV perpetrated across relationship types meant that the safeguarding and protection advice required is also different. While younger victims were likely to be subjected to online communications which may cause psychological and emotional distress (e.g., through harassment or perceived reputational damage), older victims were likely to be subjected to a campaign of abuse that was more insidious in nature and indicated a potential risk to the victim's safety or wellbeing.

Safeguarding advice to victims of all ages must be provided in a manner which does not infer blame on victims or suggest that they are in some way responsible for being victimised. This advice should recognise and reflect the fact that TFIPV perpetrators capitalise on publicly volunteered information that is freely obtainable on social media platforms. Raising awareness that TFIPV perpetrators can appropriate this available information for misuse or manipulation may inspire members of the public seek out and apply safeguarding advice.

Recommendations:

- **Privacy and safeguarding advice should be designed in an age-appropriate manner, and with specific audiences in mind, to ensure it is relevant and inclusive.**
- **Public online safety awareness campaigns should adopt an approach that does not suggest that victims are responsible for TFIPV.**
- **Relationships and Sex Education (delivered to schoolchildren across England and Wales) should include information about appropriate and healthy online behaviours in romantic relationships.**
- **Visible advice and information for all ages about healthy online behaviours and relationships should be available, and should place the onus on the perpetrator of the abusive behaviours.**

- **Advice and support should be disseminated via different mediums and platforms, and the approach tailored accordingly, to appeal to a wider audience.**
- **Practical, technology-focused education campaigns should be designed to help the general public understand the methods employed by perpetrators of TFIPV and encourage victims to better assess their own risks.**

Coordinated Responses

TFIPV, although difficult to accurately establish, shows a prevalence rate of anything from 1-80% and fits within a wider gender-based violence paradigm, especially as the predominant demographic of victims are female and perpetrators are male. This has implications for how TFIPV treated by wider society and members of the statutory sector. Experiences of TFIPV can have overt and covert impacts, but victims may be reluctant to come forward or seek help if they feel discouraged (e.g., through embarrassment, shame or self-blame). Advising victims to go offline following TFIPV will not necessarily prevent re-victimisation but does feed into victim-blaming cultures. Disengaging from online networks or digital communication settings may have an isolating impact on victims and their quality of life. It may also make them more vulnerable to TFIPV and its effects if they are unable to alert others to their (worsening) situation or seek online help and support.

Our findings illustrated a need for greater investment in multi-agency working across statutory and third-sector organisations. Understanding more about TFIPV perpetration and how to prevent or respond to it requires that TFIPV victims feel encouraged and supported to seek assistance. Victims of TFIPV are likely to present at various agencies according to the nature and immediacy of the assistance they require. Improving victim engagement by consolidating repositories of expertise will enhance multi-agency responses to TFIPV. Similarly, engaging the input of specialist domestic abuse services would address the pastoral needs of victims, allowing cyber specialist services to focus on the practical information and support necessary. Strengthening these channels of communication and interaction would also allow for improved data (evidence) collection and lessen the likelihood of the victim having to manage the situation independently.

Recommendations:

- **Specialist charities working with victims of IPV should be appropriately funded to ensure that they can comprehensively and swiftly meet the increasing demands for their services from victims of TFIPV.**
- **Cyber security specialists in the not-for-profit sector who assist victims of TFIPV should be adequately funded to ensure that they are able to continue doing so.**
- **Charities addressing sexual and domestic abuse should be encouraged to collaborate with not-for-profit cyber security organisations to improve specialist responses to TFIPV.**

- **IPV perpetrator programmes should address TFIPV. These programmes should be adequately resourced to ensure that perpetrators can access help and support to desist from violence.**

TFIPV Types and Methods

The analysis of the existing TFIPV literature indicated that TFIPV types can be broadly grouped into the following categories: Cyberstalking and Coercive Control; Harassment; Image Based Sexual Abuse; and Indirect Non-Sexual Abuse. Perpetrators employ a range of TFIPV types and methods, single incidents are rare, and most perpetrators enact more than one type of abusive behaviour towards victims. Our findings indicated the nuance of perpetrator behaviours across four key methods:

- *Unauthorised device access*: For instance, manipulating the victim's computer, phone, router, Wi-Fi network, smartwatch, home security cameras, smart home devices (baby monitor, smart TV, Amazon Alexa, etc.).
- *Tracking and monitoring*: For instance, deploying location-enabled software, spyware, keystroke logging, social media surveillance, email monitoring, (listening and recording) bugs.
- *Unwanted contact and communication*: For instance, messaging the victim directly via text, email, Wi-Fi-enabled home devices, or indirectly via own or others' social network pages, children's devices, using fake social media profiles.
- *Manipulation and control*: For instance, by interfering with the victim's private communications, blackmail and 'sextortion', impersonating the victim, gaslighting via smart home devices or email, instilling victims' fear and hyper-vigilance.

The analysis of The Cyber Helpline cases indicated that the most common type of TFIPV was *Unwanted contact and communication*, including *Cyberstalking* and *Catfishing*, followed by E*xtortion*.

Significant discrepancies were noted between victims' perceptions of TFIPV and the realities of their experiences. Helpline Responders noted that most of the victims they assisted thought that perpetrators were using sophisticated techniques to engage in TFIPV, or they believed the perpetrator to be more technologically capable. The findings of the case review did not support this belief with the most common methods of TFIPV requiring limited expertise. Nevertheless, these beliefs meant that some victims felt powerless to take action to safeguarding themselves or seek help. Victims who feel trapped or resigned may not seek help and assistance. It is important for victims to recognise that perpetrators often use readily available information, capitalise on prior access, or use proxy means of engagement (e.g., through children or shared social networks) to engage in TFIPV. Victims may have some power to impede perpetrators if they are educated about recognising these methods.

The onset of COVID-19 restrictions afforded unique opportunities which some TFIPV perpetrators capitalised on. Our findings indicated that perpetrators adapted their

approaches to continue monitoring victims using available means and methods. Prior to COVID-19 restrictions, perpetrators were more likely to employ *Technological surveillance* including monitoring internet use and spyware as well as covertly installed cameras, bugs and trackers or covert use of existing home technology. Likely due to COVID-19 restrictions some of these methods became less available to perpetrators due to a lack of physical access to passwords and devices. Post-COVID-19, perpetrators more often leveraged public information shared voluntarily by victims to engage in TFIPV.

Recommendations:

- **Public information campaigns should focus on creating more awareness about TFIPV methods and behaviours to challenge myths and stereotypes about victims and perpetrators.**
- **Greater public awareness is needed about the methods used to perpetrate TFIPV. This information should address potential points of vulnerability for victims, such as having shared passwords, being covertly recorded during video chats, or volunteering information online that perpetrators can access (e.g., on social media profiles).**
- **Information about how to secure and protect accounts needs to be kept up to date, made accessible and understandable, and should be more heavily promoted to account owners.**

Criminal Justice Responses

A degree of variability emerged regarding perceptions and experiences of criminal justice responses to TFIPV. Some police forces were commended on their approach with victims and cases, whereas a need for improvement was highlighted for others. This was attributed to the absence of a standardised approach or suitable protocol for responding to TFIPV in the UK. There are pros and cons to implementing a standardised approach to TFIPV and therefore any recommendations and actions need to take a measured approach. On the one hand, a standardisation in response means that organisations like The Cyber Helpline will be more aware of the policies and procedures guiding statutory involvement in TFIPV cases and can act accordingly. On the other hand, the variable and evolving nature of TFIPV means that a standardised approach may prove less effective if the type of abuse has evolved to encompass behaviours that are beyond the remit of any demarcated policies and practices. Also, standardising approaches requires a level of investment, capacity-building, resourcing, training and operational management that may be beyond the scope of some police forces' budgets.

Collecting evidence of TFIPV may also prove difficult without clear policies outlining who is responsible for collection and how it should be done. If victims are advised to delete malicious communications from their devices or employ factory resets, this may impede the effective investigation of crimes committed against them. Malicious communications may constitute evidence; therefore the victims are required to retain them as evidence. However, it should

be recognised that keeping distressing communications for evidential purposes may cause victims additional disconcert and impede their ability to move on from the experience.

Recommendations:

- **Police officers should have access to relevant, specialist training to improve their capacity to recognise and respond to TFIPV victims and incidents.**
- **Police forces should be appropriately and consistently funded to ensure they have the capacity to provide a robust response to TFIPV (e.g., assistance in appropriate gathering of digital evidence).**
- **Consideration should be given to implementing a standardised (national) response to TFIPV, applicable to all regional police forces, to assist with evidence collection and investigation practices.**
- **Swift and proportionate sanctions, which are commensurate with existing IPV offences, should be imposed upon perpetrators.**
- **Victims who report TFIPV should be kept informed of developments in their case. They should also be advised accordingly with regards to the potential variability and intensification of TFIPV methods they may encounter.**

Ensuring Accountability

Many TFIPV perpetrators were considered as acting with relative impunity, given that most appeared to encounter very few impediments or repercussions. The anonymity afforded by the Internet, coupled with the lack of enforced sanctions against TFIPV perpetrators, enables them to engage in periods of prolonged and unimpeded harassment of victims. Being able to harass with impunity meant some perpetrators escalated their TFIPV behaviours against victims, while others honed their techniques during subsequent relationships. Additionally, those who may have felt justified in their rationales or behaviours were unlikely to desist without some form of external or regulatory intervention. Therefore, while holding perpetrators to account is important, it is also necessary to ensure that effective impediments are in place to curtail their ability to continue abusing victims.

Helpline Responders identified several problems with how social media companies and technology organisations deal with TFIPV. These included only using an automated service to interact with victims who report abuse; extensive delays in acting or responding to such reports; failing to block perpetrators from setting up new or fake accounts to harass victims; and rendering users vulnerable through confusing or opaque updates of privacy and security settings. These issues require attention to improve the assistance provided to victims while impeding perpetrators from beginning or continuing to engage in TFIPV.

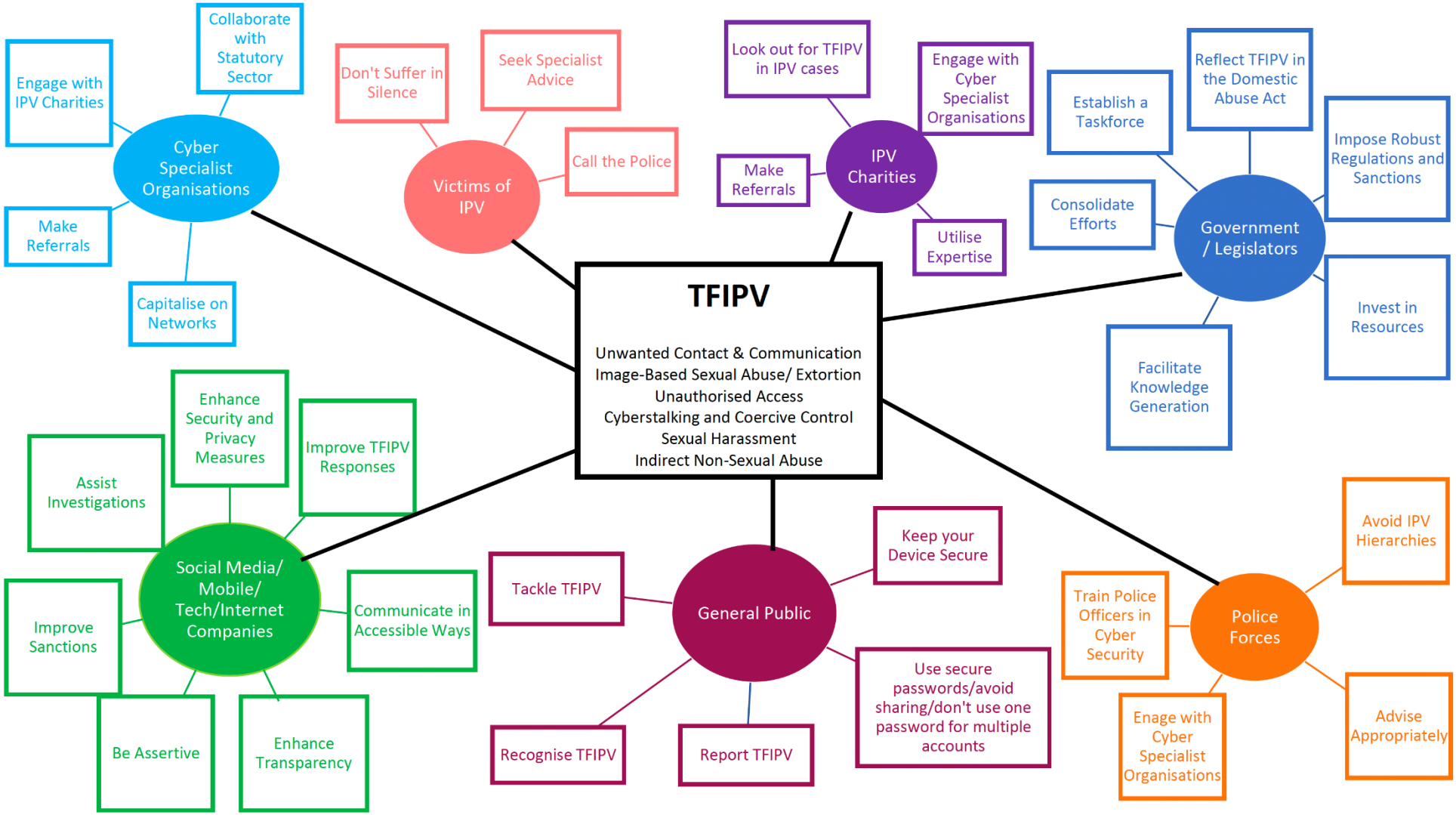
Recommendations:

- **Online providers and social media platforms should clearly outline to users how they will respond to reported TFIPV and what sanctions they impose on perpetrators.**

- **Information about how to implement or check privacy and security settings should be communicated to users in a format which is straightforward, accessible and easily located.**
- **Privacy and security settings for devices and accounts should be communicated to users in a format which is straightforward, accessible and easily located to improve understanding of implications and to allow verification.**
- **Device manufacturers and online service providers should ensure that enhanced security settings, such as two-factor authentication or account ID verification, are enabled as standard/default on devices and accounts.**
- **Providers should enable users to easily audit who has been connecting to their home Wi-Fi network as well as who has been accessing their accounts or devices.**
- **The Government should ensure that online providers and tech organisations are appropriately regulated. This should involve updating legislation to impose sanctions and reinforce accountability among service providers to ensure users are safeguarded and their engagement with online platforms is safe.**

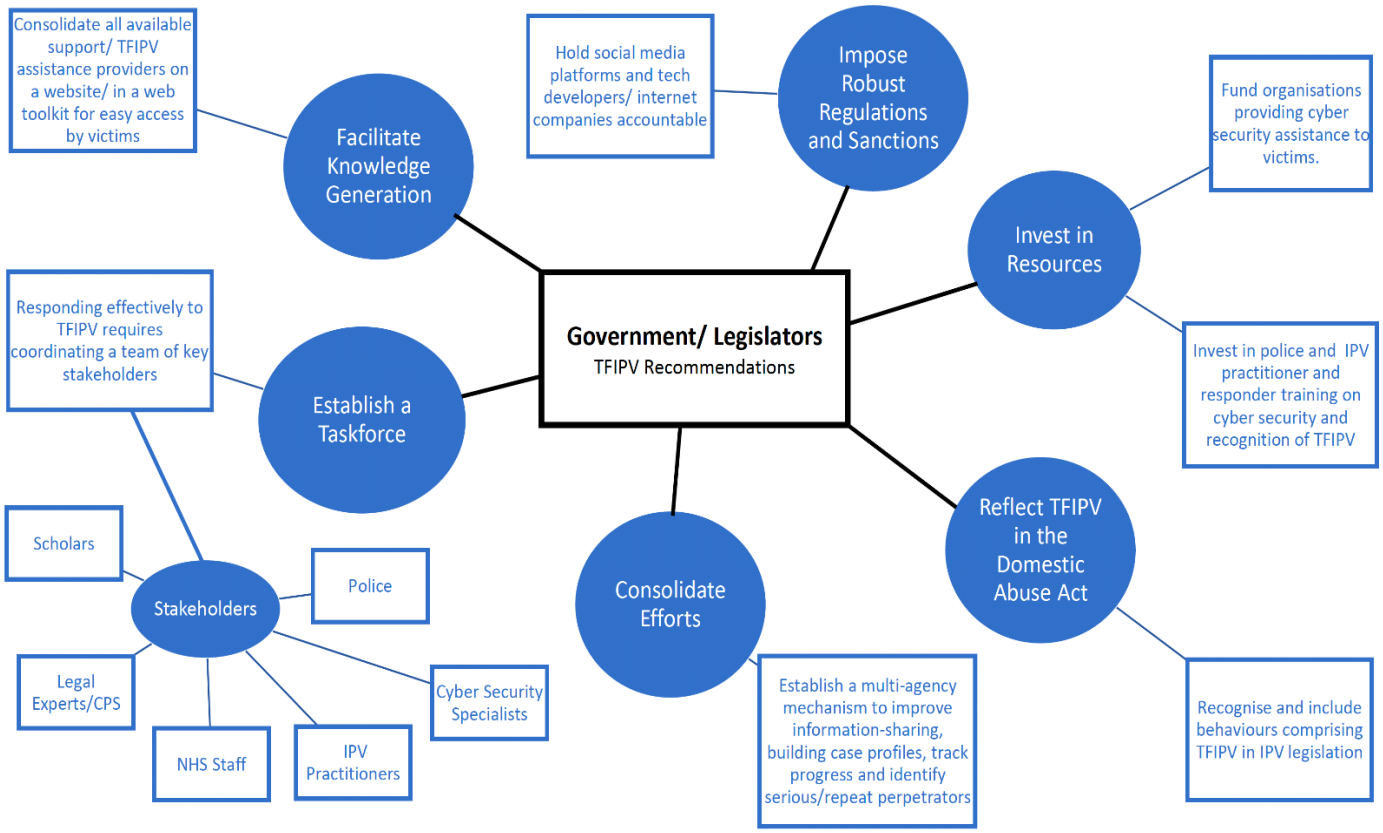
Tackling TFIPV Toolkit

Based on our consolidated research findings, here are our specific suggestions for actions that can help various stakeholders recognise, respond to, and reduce TFIPV perpetration.


TFIPV
Unwanted Contact & Communication
Image-Based Sexual Abuse/ Extortion
Unauthorised Access
Cyberstalking and Coercive Control
Sexual Harassment
Indirect Non-Sexual Abuse
Cyber Specialist Organisations
Collaborate with Statutory Sector
Engage with IPV Charities
Make Referrals
Capitalise on Networks
Victims of IPV
Don't Suffer in Silence
Seek Specialist Advice
Call the Police
IPV Charities
Look out for TFIPV in IPV cases
Engage with Cyber Specialist Organisations
Make Referrals
Utilise Expertise
Government / Legislators
Establish a Taskforce
Reflect TFIPV in the Domestic Abuse Act
Impose Robust Regulations and Sanctions
Consolidate Efforts
Invest in Resources
Facilitate Knowledge Generation
Social Media/ Mobile/ Tech/Internet Companies
Enhance Security and Privacy Measures
Improve TFIPV Responses
Assist Investigations
Improve Sanctions
Communicate in Accessible Ways
Be Assertive
Enhance Transparency
General Public
Tackle TFIPV
Keep your Device Secure
Use secure passwords/avoid sharing/don't use one password for multiple accounts
Recognise TFIPV
Report TFIPV
Police Forces
Avoid IPV Hierarchies
Train Police Officers in Cyber Security
Advise Appropriately
Enage with Cyber Specialist Organisations

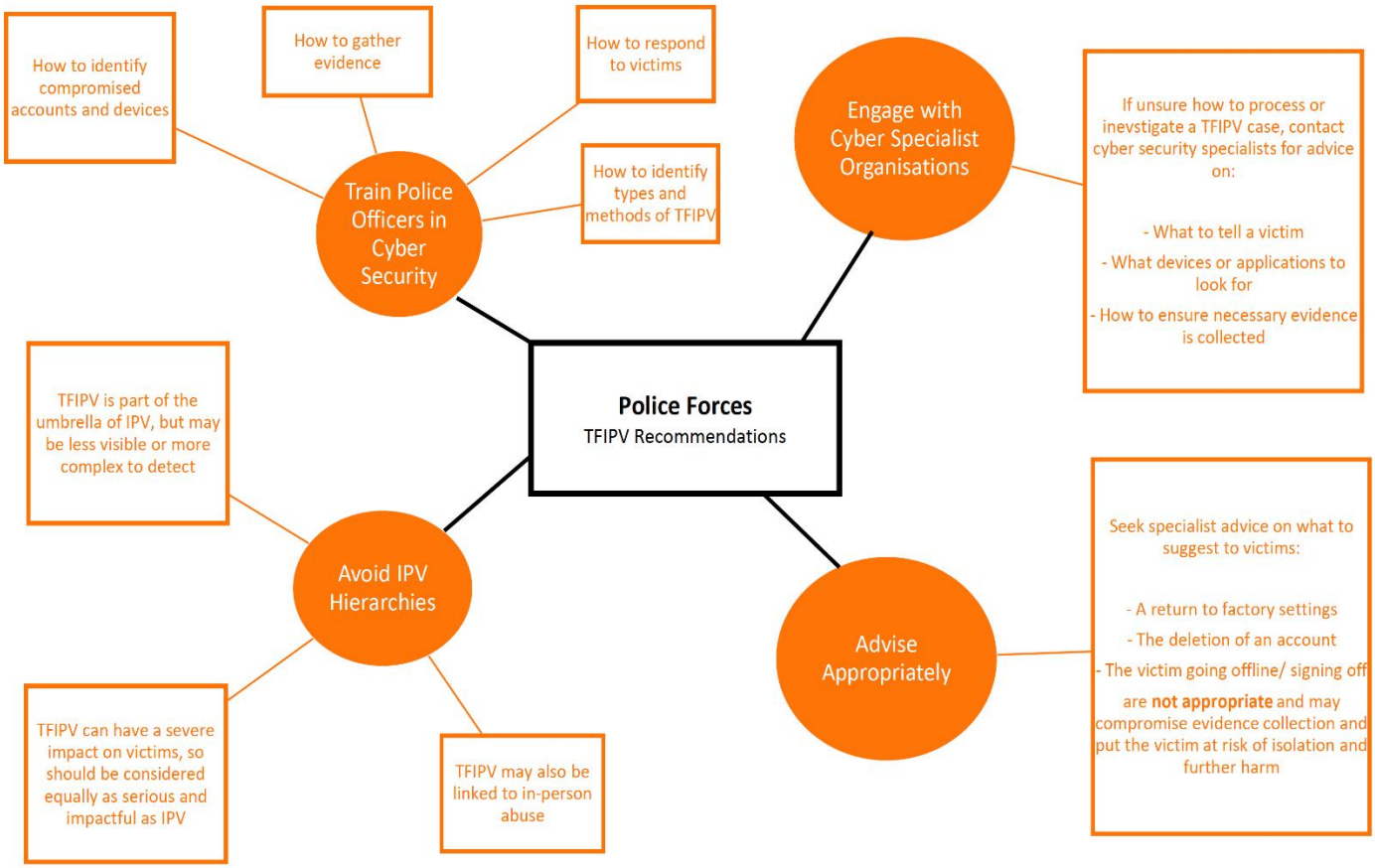
Government/Legislators

- *Reflect TFIPV in the Domestic Abuse Act*: Recognise behaviours comprising TFIPV in legislation as part of IPV and coercive control.
- *Impose robust regulations and sanctions*: Help to combat TFIPV by holding social media platforms and tech developers and companies accountable.
- *Invest in resources*: Fund organisations to provide cyber security assistance to victims. Invest in police and IPV practitioner and responder training on cyber security and recognition of TFIPV.
- *Facilitate knowledge generation*: Collect contact information for all available support and assistance providers for TFIPV and list this on one website or web-toolkit for easy access by victims.
- *Consolidate efforts*: Establish a multi-agency reporting mechanism to improve information-sharing, build case profiles, track progress and identify serious or repeat perpetrators.
- *Establish a taskforce*: Coordinate a team of key stakeholders comprised of police, cyber security specialists, IPV practitioners, NHS staff, legal experts and scholars to provide strategic leadership in efforts to combat TFIPV.



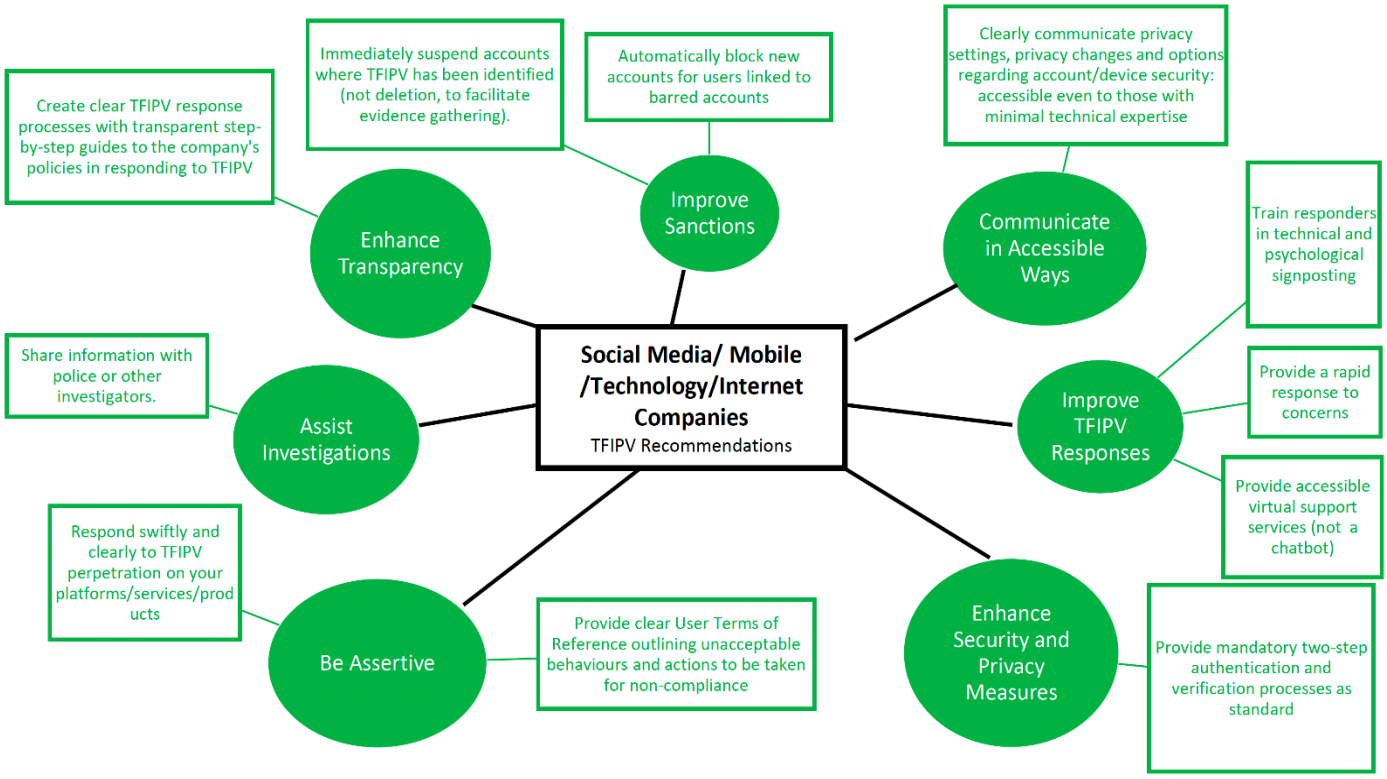
Police Forces

- *Avoid IPV hierarchies*: Consider TFIPV part of the wider umbrella of IPV, even though it may be less visible or more complicated to detect. TFIPV can have severe impacts on victims, and may also be linked to in-person abuse, therefore should be considered equally as serious and impactful as offline IPV.
- *Advise appropriately*: Seek specialist advice about unfamiliar technologies or online behaviours. Suggesting that victims restore factory settings, delete accounts, or go offline may compromise important evidence and put them at further risk (e.g., if the perpetrator suspects that the victim is trying to leave or report the abuse).
- *Engage with cyber specialist organisations*: Use available experts to advise on how to process or investigate a TFIPV case. Cyber security specialists can outline to obtain advice on what to tell a victim, what devices or applications to look for and how to ensure that necessary evidence is collected.
- *Train police officers in cyber security*: Equip officers with the knowledge and confidence to recognise available types and methods of TFIPV. Being able to identify compromised accounts and devices will assist officers in gathering evidence and responding to victims.



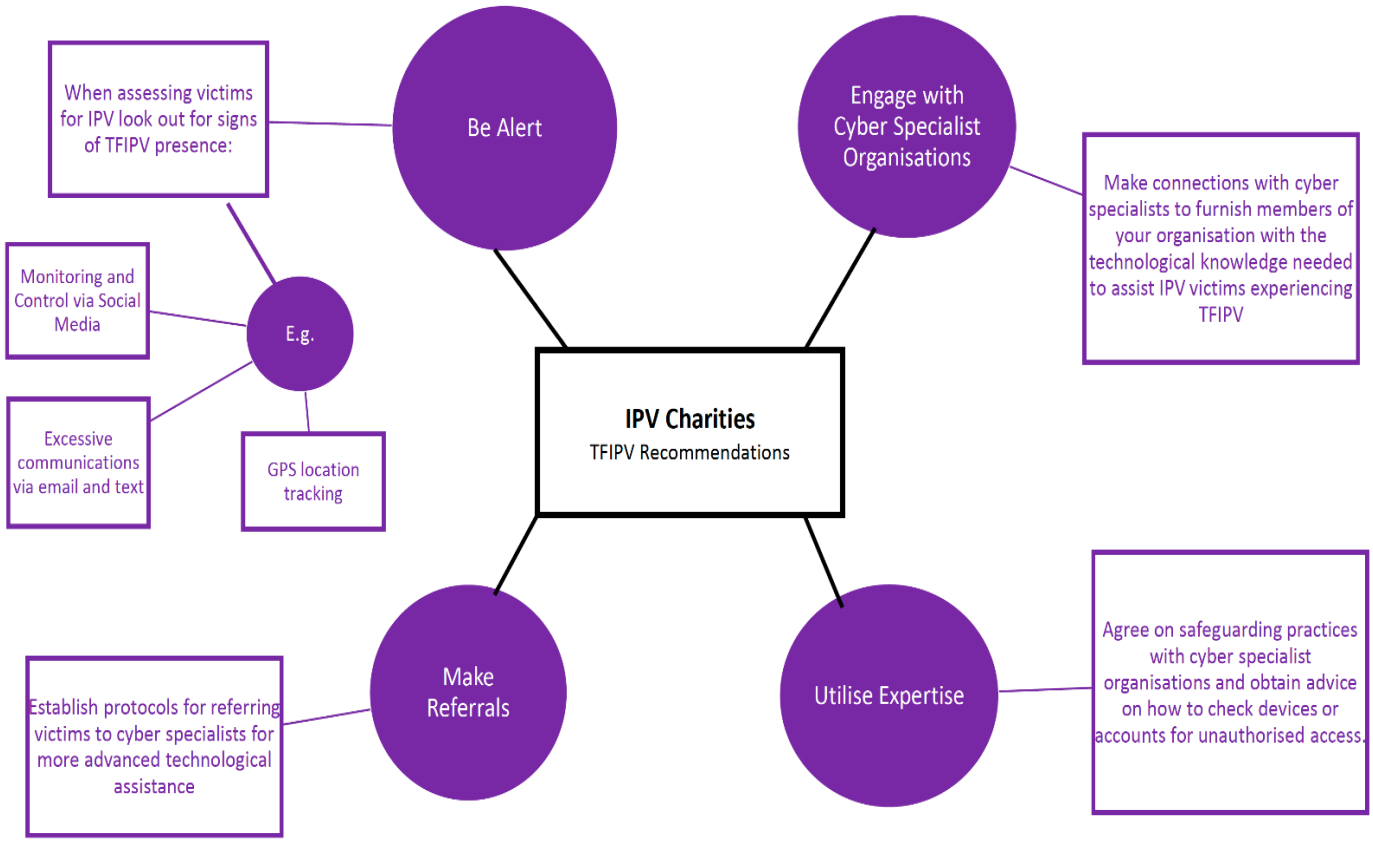
Social Media / Mobile / Technology Companies /Internet Providers

- *Enhance security and privacy measures*: Increase the mandatory application of two-factor or multi-factor authentication and verification processes as standard with all devices and accounts.
- *Improve TFIPV responses*: Respond to concerned users as soon as possible, give them the option to speak to someone virtually (not a chatbot) and train responders to be able to offer appropriate technical and psychological signposting.
- *Communicate in accessible ways*: Clearly communicate privacy settings, privacy changes and options regarding the security of an account or device to service users, in a way that is easily understood even by those who have minimal technical expertise.
- *Enhance transparency*: Inform users about your commitment to combating TFIPV and other online abuse. Provide a transparent step-by-step guide of your company's processes for dealing with reports of abuse.
- *Be assertive*: Have a clear and swift response to the perpetration of abuse detected or reported on your platforms. User Terms of Reference should be clear on what behaviours will not be tolerated and what happens to those who transgress.
- *Improve sanctions*: Take swift action. Upon identifying potential TFIPV perpetrators, accounts should immediately be suspended, not deleted, (to facilitate the ability to gather evidence). Automatically block new accounts by users providing details or email addresses linked to barred accounts.
- *Assist investigations*: Share available or known information that could help with a case.



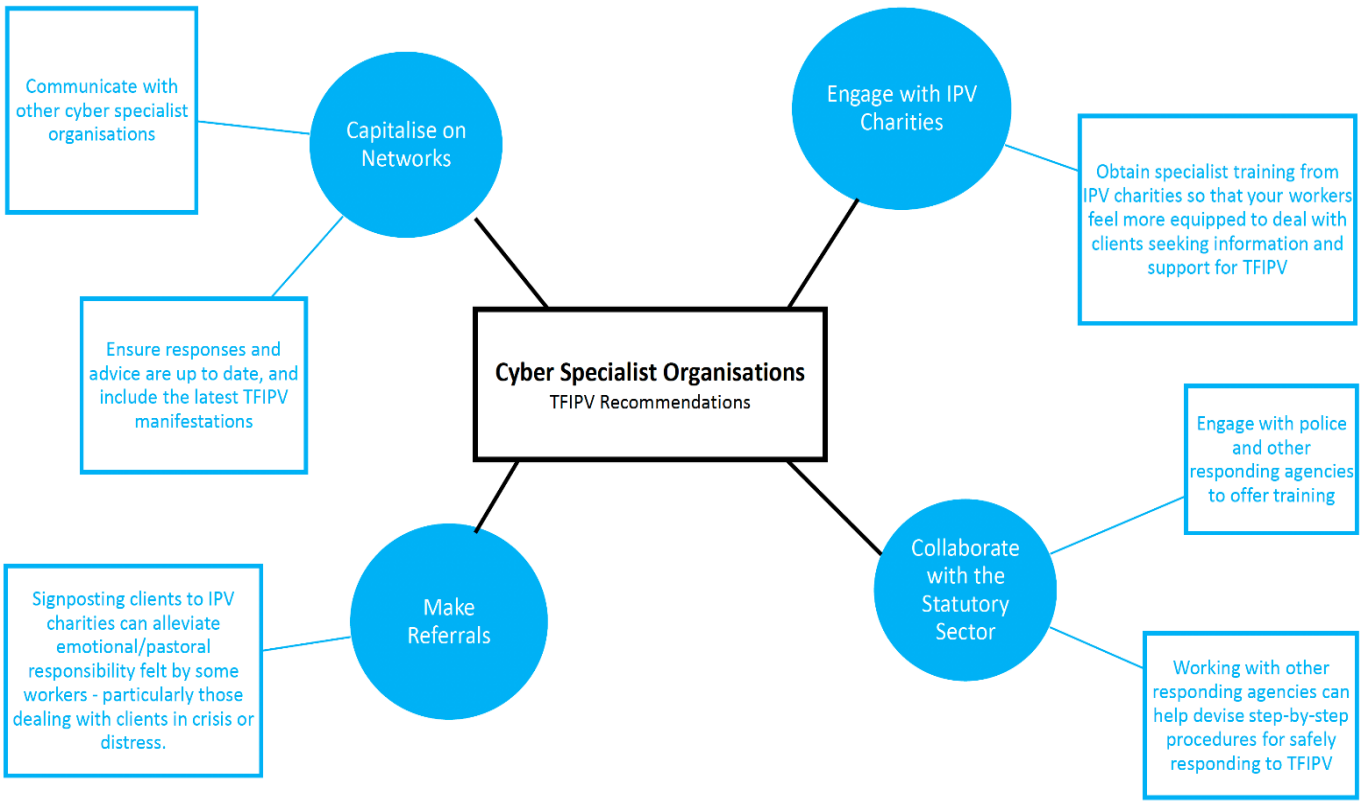
IPV Charities

- *Engage with cyber specialist organisations*: Make connections with cyber specialists to furnish members of your organisation with the level of technological knowledge that you need to assist IPV victims who disclose that they are experiencing TFIPV.
- *Utilise expertise*: Agree on safeguarding practices with cyber specialist organisations and obtain advice on how to check devices or accounts for unauthorised access.
- *Make referrals*: Establish protocols for referring victims to cyber specialists for more advanced technological assistance.
- *Be alert*: When risk assessing IPV victims, look out for signs of TFIPV such as monitoring and control via social media, excessive communications via email and text, GPS location tracking etc.



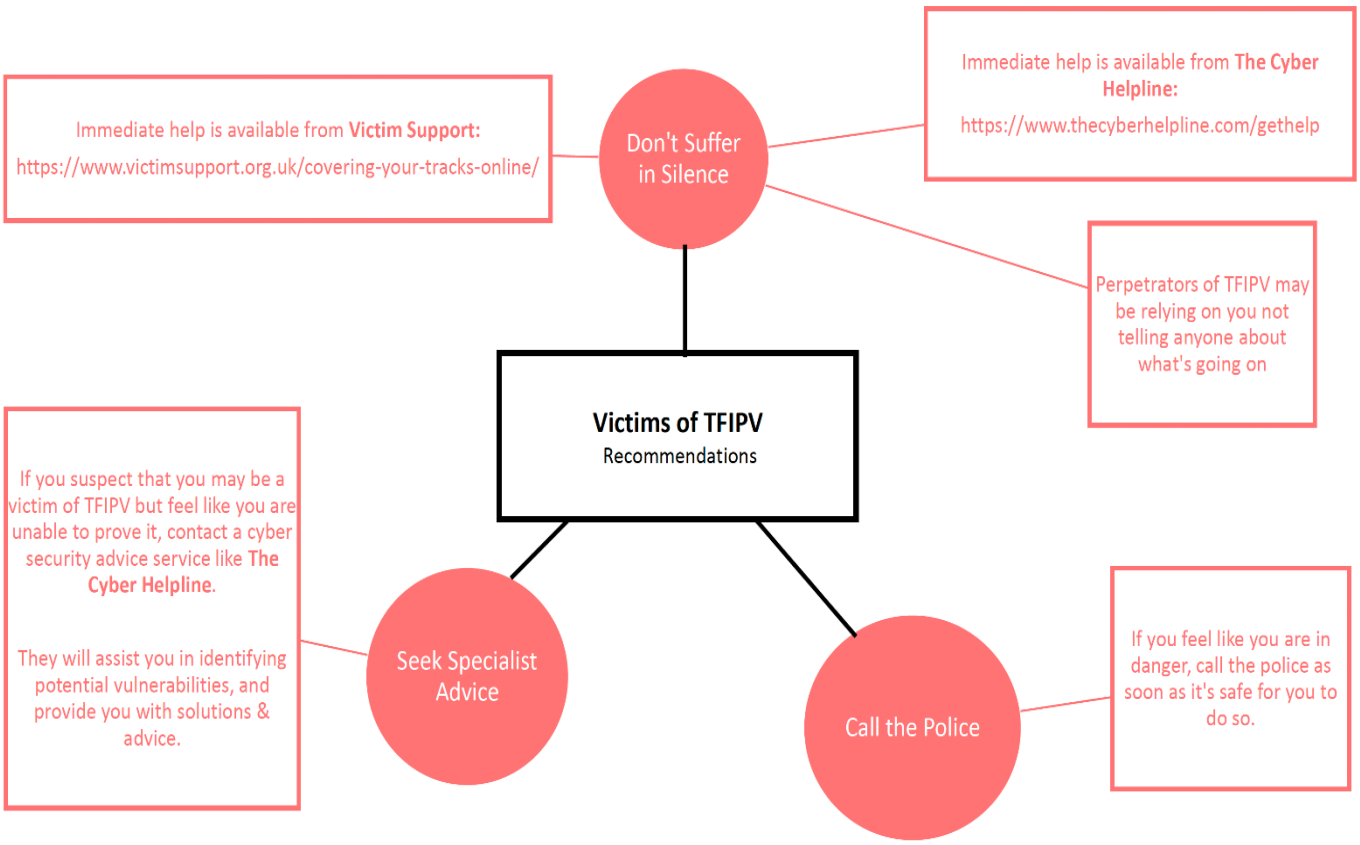
Cyber Specialist Organisations (corporate and not-for-profit)

- *Engage with IPV charities*: Obtain specialist training from IPV charities to ensure that your workers feel more equipped to deal with clients who are seeking information and support for TFIPV.
- *Make referrals*: Signposting clients to IPV charities can also alleviate some of the emotional and pastoral responsibility felt by some workers, particularly those who are dealing with clients in crisis situations or distressed states.
- *Collaborate with the statutory sector*: Engage with the police and other responding agencies to offer training. Working together can help to devise step-by-step procedures for safely responding to TFIPV.
- *Capitalise on networks*: Communicate with other cyber specialist organisations to ensure that responses and advice are up to date and include all latest manifestations of TFIPV.



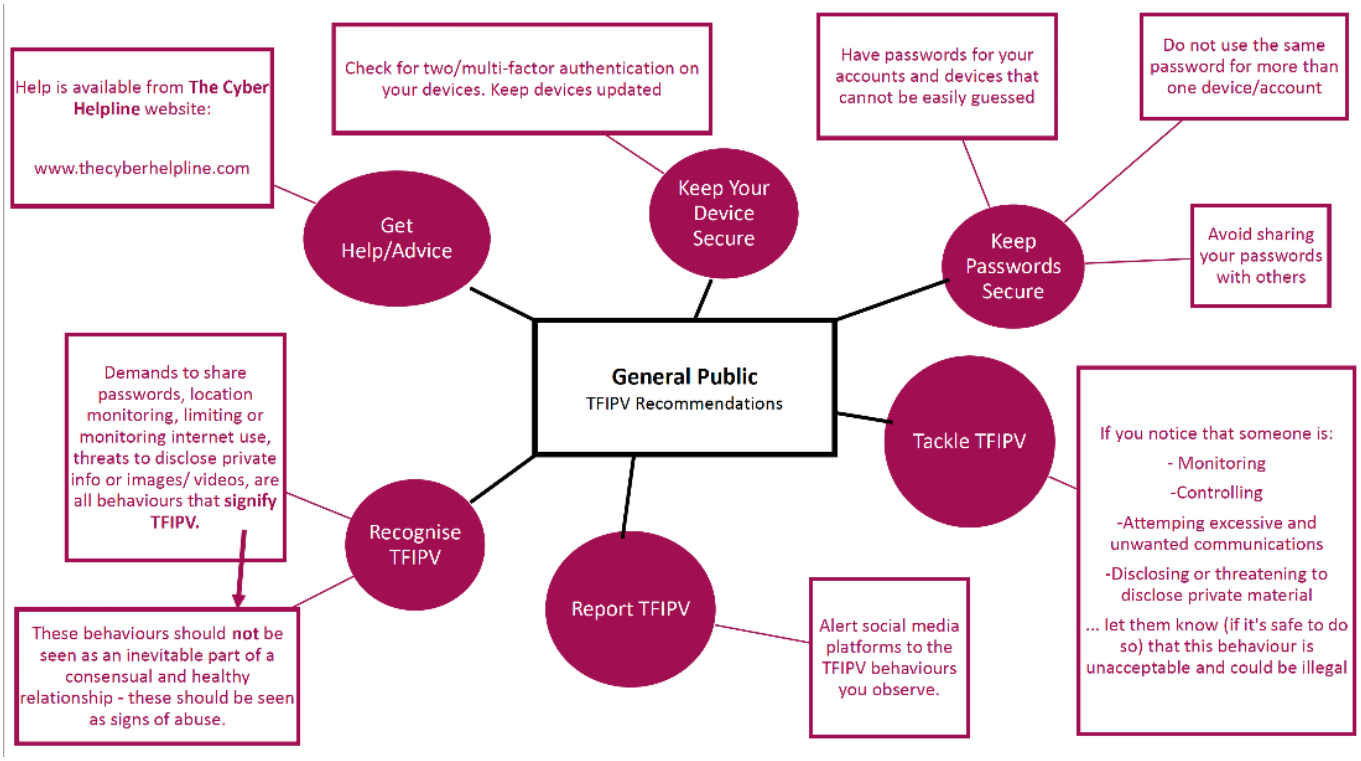
Victims of TFIPV

- *Don't suffer in silence*: Perpetrators of TFIPV may be relying on you not telling anyone about what is going on. There is immediate help and advice available from The Cyber Helpline (https://www.thecyberhelpline.com/gethelp) and Victim Support (https://www.victimsupport.org.uk/covering-your-tracks-online/)
- *Call the police*: If you feel like you are in danger, call the police as soon as it is safe for you to do so.
- *Seek specialist advice*: If you suspect that you may be a victim of TFIPV, but feel like you are unable to prove it, you should contact a cyber security advice service like The Cyber Helpline: they will assist you in identifying potential vulnerabilities and provide you with solutions and advice.



General Public

- *Recognise TFIPV*: Demands to share passwords, location monitoring, limiting or monitoring someone's Internet use, knowledge of undisclosed personal information, threats to disclose private information or images/videos of someone, are all behaviours that signify TFIPV. These behaviours should not be seen as an inevitable part of a consensual and healthy relationship and should be seen as signs of abuse.
- *Tackle TFIPV*: You may be aware of someone who is monitoring, controlling, attempting excessive and unwanted communications, disclosing or threatening to disclose private material or classified information about someone else. These behaviours are unacceptable may be prohibited by law. If you can, and if it is safe for you to do so, speak to the person who is demonstrating these behaviours to indicate that they are not acceptable and can also be illegal.
- *Report TFIPV*: Use available reporting mechanisms to alert social media platforms to the TFIPV behaviours you observe. You do not have to be the victim to make a report, you can do this as a third-party observer (e.g., if you witness behaviours being perpetrated by or against someone else).
- *Keep your device secure*: Check for two- or multi-factor authentication on your devices. Keep your devices updated: manufacturers will often release security updates but these may require you to install and/or enable them.
- *Keep your passwords secure*: Protect yourself using strong passwords for your devices and accounts that cannot be easily guessed and that only you know. Where possible avoid sharing your passwords with others and using the same password for multiple accounts.



References:

Al-Alosi, H. (2017). *CYBER-VIOLENCE: DIGITAL ABUSE IN THE CONTEXT OF DOMESTIC VIOLENCE*. http://www.abc.net.au/

Alshehri, A., Salem, M. ben, & Ding, L. (2020). Are smart home devices abandoning IPV victims? *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, 1368–1375. https://doi.org/10.1109/TrustCom50675.2020.00184

Attrill-Smith, A. & Wesson, C. (2020). *The psychology of cybercrime.* In T. J. Holt & A. M. Bossler (Eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave McMillan https://doi.org/10.1007/978-3-319-78440-3

Bellini, R., Tseng, E., McDonald, N., Greenstadt, R., McCoy, D., Ristenpart, T., & Dell, N. (2021). "So-called privacy breeds evil." *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW3), 1–27. https://doi.org/10.1145/3432909

Bhogal, M. S., Rhead, C., & Tudor, C. (2019). Understanding digital dating abuse from an evolutionary perspective: Further evidence for the role of mate value discrepancy. *Personality and Individual Differences*, *151*. https://doi.org/10.1016/j.paid.2019.109552

Borrajo, E., Gámez-Guadix, M., & Calvete, E. (2015a). Cyber dating abuse: Prevalence, context, and relationship with offline dating aggression. *Psychological Reports*, *116*(2), 565–585. https://doi.org/10.2466/21.16.PR0.116k22w4

Borrajo, E., Gámez-Guadix, M., & Calvete, E. (2015b). *P s i c o t h e m a Justification beliefs of violence, myths about love and cyber dating abuse*. *27*(4), 3. https://doi.org/10.7334/pslcothema2015.59

Branson, M., & March, E. (2021). Dangerous dating in the digital age: Jealousy, hostility, narcissism, and psychopathy as predictors of Cyber Dating Abuse. *Computers in Human Behavior*, *119*. https://doi.org/10.1016/j.chb.2021.106711

Brem, M. J., Florimbio, A. R., Grigorian, H., Wolford-Clevenger, C., Elmquist, J. A., Shorey, R. C., Rothman, E. F., Temple, J. R., & Stuart, G. L. (2019). Cyber abuse among men arrested for domestic violence: Cyber monitoring moderates the relationship between alcohol problems and intimate partner violence. *Psychology of Violence*, *9*(4), 410–418. https://doi.org/10.1037/vio0000130

Brem, M. J., Spiller, L. C., & Vandehey, M. A. (2015). Online Mate-Retention Tactics on Facebook Are Associated With Relationship Aggression. *Journal of Interpersonal Violence*, *30*(16), 2831–2850. https://doi.org/10.1177/0886260514554286

Brown, A. (2017). What is so special about online (as compared to offline) hate speech? *Ethnicities, 18*(3), 297-236

Brown, C., Flood, M. and Hegarty, K. (2020) 'Digital dating abuse perpetration and impact: The importance of gender', *Journal of Youth Studies*, 0(0), pp. 1–16. doi: 10.1080/13676261.2020.1858041.

Brown, C., & Hegarty, K. (2018). Digital dating abuse measures: A critical review. In *Aggression and Violent Behavior* (Vol. 40, pp. 44–59). Elsevier Ltd. https://doi.org/10.1016/j.avb.2018.03.003

Brown, C., & Hegarty, K. (2021). Development and validation of the TAR Scale: A measure of technology-facilitated abuse in relationships. *Computers in Human Behavior Reports*, *3*, 100059. https://doi.org/10.1016/j.chbr.2021.100059

Brown, M. L., Reed, L. A., & Messing, J. T. (2018). Technology based abuse: Intimate partner violence and the use of information communication technologies. In J. R. Vickery & T. Everbach (Eds.), Mediating misogyny: Gender, technology, and harassment (pp. 209–227). Springer International Publishing.

Bui, N. H., & Pasalich, D. S. (2021). Insecure Attachment, Maladaptive Personality Traits, and the Perpetration of In-Person and Cyber Psychological Abuse. *Journal of Interpersonal Violence*, *36*(5–6), 2117–2139. https://doi.org/10.1177/0886260518760332

Burke, S. C., Wallen, W., Vail-Smith, K. & Knox, D. (2011). 'Using technology to control intimate partners: An exploratory study of college undergraduates', *Computers in Human Behavior*, 27(3), pp. 1162–1167. doi: 10.1016/j.chb.2010.12.010.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Routledge. https://doi.org/10.4324/9780203771587

Campbell, A. M. (2020). An increasing risk of family violence during the Covid-19 pandemic: Strenghtening community collaborations to save lives. *Forensic Science International Reports (2)* doi: 10.1016/j.fsir.2020.100089

Cantu, J. I., & Charak, R. (2020). Unique, Additive, and Interactive Effects of Types of Intimate Partner Cybervictimization on Depression in Hispanic Emerging Adults. *Journal of Interpersonal Violence*. https://doi.org/10.1177/0886260520915552

Caridade, S., Braga, T., & Borrajo, E. (2019). Cyber dating abuse (CDA): Evidence from a systematic review. In *Aggression and Violent Behavior* (Vol. 48, pp. 152–168). Elsevier Ltd. https://doi.org/10.1016/j.avb.2019.08.018

Caridade, S., Pedrosa e Sousa, H. F. and Dinis, M. A. P. (2020) 'Cyber and offline dating abuse in a portuguese sample: Prevalence and context of abuse', *Behavioral Sciences*, 10(10), pp. 1–14. doi: 10.3390/BS10100152.

Charak, R., Villareal, L., Schmitz, R. M., Hirai, M., & Ford, J. D. (2019) 'Patterns of childhood maltreatment and intimate partner violence, emotion dysregulation, and mental health symptoms among lesbian, gay, and bisexual emerging adults: A three-step latent class approach', *Child Abuse and Neglect*, 89(December 2018), pp. 99–110. doi: 10.1016/j.chiabu.2019.01.007.

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., & Ristenpart, T. (2018). The Spyware Used in Intimate Partner Violence. *Proceedings - IEEE Symposium on Security and Privacy*, *2018-May*, 441–458. https://doi.org/10.1109/SP.2018.00061

Christie, L., & Wright, S (2020). Technology and domestic abuse. Rapid response post for the UK Parliament. https://post.parliament.uk/technology-and-domestic-abuse/

Clevenger, S., & Gilliam, M. (2020). *Intimate Partner Violence and the Internet: Perspectives.* In T. J. Holt & A. M. Bossler (Eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave McMillan https://doi.org/10.1007/978-3-319-78440-3

Crane, C. A., Umehira, N., Berbary, C., & Easton, C. J. (2018). Problematic alcohol use as a risk factor for cyber aggression within romantic relationships. *American Journal on Addictions*, *27*(5), 400–406. https://doi.org/10.1111/ajad.12736

Crown Prosecution Service (2019). *Annual Violence Against Women and Girls Report* https://www.cps.gov.uk/cps/news/annual-violence-against-women-and-girls-report-published-0

Crown Prosecution Service (2020). *Stalking analysis reveals domestic abuse link* https://www.cps.gov.uk/cps/news/stalking-analysis-reveals-domestic-abuse-link

Cybersmile Foundation, The (2017). Stop Cyberbullying Day Survey 2017 report. https://www.cybersmile.org/wp-content/uploads/Stop-Cyberbullying-Day-Survey-2017.pdf

Dardis, C. M., & Gidycz, C. A. (2019). Reconciliation or retaliation? An integrative model of postrelationship in-person and cyber unwanted pursuit perpetration among undergraduate men and women. *Psychology of Violence*, *9*(3), 328–339. https://doi.org/10.1037/vio0000102

Davidson, J., Livingstone, S., Jenkins, S., Gekoski, A., Choak, C., Ike, T. & Phillips, K. (2019). Adult Online Hate, Harassment and Abuse: A Rapid Evidence Assessment. UK Council for Internet Safety https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf

Deans, H. and Bhogal, M. S. (2019) 'Perpetrating Cyber Dating Abuse: A Brief Report on the Role of Aggression, Romantic Jealousy and Gender', *Current Psychology*, 38(5), pp. 1077–1082. doi: 10.1007/s12144-017-9715-4.

DeKeseredy, W. S., Schwartz, M. D., Harris, B., Woodlock, D., Nolan, J. & Hall-Sanchez, A. (2019). Technology-facilitated stalking and unwanted sexual messages/images in a college campus community: The role of negative peer support. *Sage Open* *9*(1). https://doi.org/10.1177/2158244019828231

Department of Digital, Culture, Media & Sport and Home Office (2019). Online Harms White Paper. https://www.gov.uk/government/consultations/online-harms-white-paper

Department of Digital, Culture, Media & Sport and Home Office (2020). Consultation Outcome: Online Harms White Paper. https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper

Dimond, J. P., Fiesler, C. and Bruckman, A. S. (2011) 'Domestic violence and information communication technologies', *Interacting with Computers*, 23(5), pp. 413–421. doi: 10.1016/j.intcom.2011.04.006.

Domestic Abuse Act (2021). https://www.legislation.gov.uk/ukpga/2021/17/contents/enacted

Domestic Violence Resource Centre Victoria (DVRCV; 2013). Smart Safe. https://dvrcv.org.au/smartsafe

Doucette, H., Collibee, C., Hood, E., Stone, D. I. G., DeJesus, B. & Rizzo, C. D. (2018). 'Perpetration of Electronic Intrusiveness Among Adolescent Females: Associations With In-Person Dating Violence', *Journal of Interpersonal Violence*. doi: 10.1177/0886260518815725.

Douglas, H., Harris, B. A. and Dragiewicz, M. (2019) 'Technology-facilitated domestic and family violence: Women's experiences', *British Journal of Criminology*, 59(3), pp. 551–570. doi: 10.1093/bjc/azy068.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, *18*(4), 609–625. https://doi.org/10.1080/14680777.2018.1447341

Drouin, M., Ross, J., & Tobin, E. (2015). Sexting: A new, digital vehicle for intimate partner aggression? *Computers in Human Behavior*, *50*, 197–204. https://doi.org/10.1016/j.chb.2015.04.001

Duerksen, K. N., & Woodin, E. M. (2019a). Cyber Dating Abuse Victimization: Links With Psychosocial Functioning. *Journal of Interpersonal Violence*. https://doi.org/10.1177/0886260519872982

Duerksen, K. N., & Woodin, E. M. (2019b). Technological intimate partner violence: Exploring technology-related perpetration factors and overlap with in-person intimate partner violence. *Computers in Human Behavior*, *98*, 223–231. https://doi.org/10.1016/j.chb.2019.05.001

Duncan, Z., & March, E. (2019). Using Tinder® to start a fire: Predicting antisocial use of Tinder® with gender and the Dark Tetrad. *Personality and Individual Differences*, *145*, 9–14. https://doi.org/10.1016/j.paid.2019.03.014

EFSA (2017). *Guidance on the use of the weight of evidence approach in scientific assessments*

https://doi.org/10.2903/j.efsa.2017.4971

Ellyson, A. M., Adhia, A., Lyons, V. H., & Rivara, F. P. (2021) 'Prevalence, age of initiation, and patterns of co-occurrence of digital dating abuse behaviors nationwide', *Children and Youth Services Review*, 122(December 2020), p. 105921. doi: 10.1016/j.childyouth.2020.105921.

Eterovic-Soric, B., Choo, K. K. R., Ashman, H., & Mubarak, S. (2017). Stalking the stalkers – detecting and deterring stalking behaviours using technology: A review. In *Computers and Security* (Vol. 70, pp. 278–289). Elsevier Ltd. https://doi.org/10.1016/j.cose.2017.06.008

Fernet, M., Lapierre, A., Hébert, M., & Cousineau, M. M. (2019). A systematic review of literature on cyber intimate partner victimization in adolescent girls and women. In *Computers in Human Behavior* (Vol. 100, pp. 11–25). Elsevier Ltd. https://doi.org/10.1016/j.chb.2019.06.005

Flach, R. M. D., & Deslandes, S. F. (2017). Abuso digital en relaciones afectivo-sexuales: Un análisis bibliográfico. In *Cadernos de Saude Publica* (Vol. 33, Issue 7). Fundacao Oswaldo Cruz. https://doi.org/10.1590/0102-311X00138516

Flach, R. M. D., & Deslandes, S. F. (2019). Cyber dating abuse or proof of love? The use of apps for surveillance and control in affective-sexual relations. *Cadernos de Saude Publica*, *35*(1). https://doi.org/10.1590/0102-311x00060118

Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T., & Dell, N. (2019). "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW). https://doi.org/10.1145/3359304

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A stalker's paradise": How intimate partner abusers exploit technology. *Conference on Human Factors in Computing Systems - Proceedings*, *2018-April*. https://doi.org/10.1145/3173574.3174241

Gilchrist, G., Canfield, M., Radcliffe, P., & D'Oliveira, A. F. P. L. (2017). Controlling behaviours and technology-facilitated abuse perpetrated by men receiving substance use treatment in England and Brazil: Prevalence and risk factors. *Drug and Alcohol Review*, *36*(1), 52–63. https://doi.org/10.1111/dar.12521

Global News Canada (2020). LAWS reports "alarming" surge in demand for services during COVID-19. https://globalnews.ca/news/7764058/lawc-alarming-surge-demand-services-covid-19-pandemic/

Gracia-Leiva, M., Puente-Martínez, A., Ubillos-Landa, S., González-Castro, J. L., & Páez-Rovira, D. (2020). Off- and online heterosexual dating violence, perceived attachment to parents and peers and suicide risk in young women. *International Journal of Environmental Research and Public Health*, *17*(9). https://doi.org/10.3390/ijerph17093174

Grimani, A., Gavine, A., & Moncur, W. (2020). An Evidence Synthesis of Covert Online Strategies Regarding Intimate Partner Violence. In *Trauma, Violence, and Abuse*. SAGE Publications Ltd. https://doi.org/10.1177/1524838020957985

Hancock, K., Keast, H. and Ellis, W. (2017) 'The impact of cyber dating abuse on self-esteem: The mediating role of emotional distress', *Cyberpsychology*, 11(2). doi: 10.5817/CP2017-2-2.

Harkin, D., & Molnar, A. (2020). Operating-System Design and Its Implications for Victims of Family Violence: The Comparative Threat of Smart Phone Spyware for Android Versus iPhone Users. *Violence Against Women*. https://doi.org/10.1177/1077801220923731

Harkin, D., Molnar, A., & Vowles, E. (2020). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, Media, Culture*, *16*(1), 33–60. https://doi.org/10.1177/1741659018820562

Harris, B. A., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *British Journal of Criminology*, *59*(3), 530–550. https://doi.org/10.1093/bjc/azy052

Havron, S., Freed, D., Chatterjee, R., Tech, C., Mccoy, D., Dell, N., & Ristenpart, T. (2019). *Clinical Computer Security for Victims of Intimate Partner Violence*. https://www.usenix.org/system/files/sec19-havron.pdf

Hellevik, P. M. (2019) 'Teenagers' personal accounts of experiences with digital intimate partner violence and abuse', *Computers in Human Behavior*, 92(November 2018), pp. 178–187. doi: 10.1016/j.chb.2018.11.019.

Henry, N., Flynn, A. and Powell, A. (2018) 'Policing image-based sexual abuse: stakeholder perspectives', *Police Practice and Research*, 19(6), pp. 565–581. doi: 10.1080/15614263.2018.1507892.

Henry, N., Flynn, A., & Powell, A. (2020). Technology-Facilitated Domestic and Sexual Violence: A Review. *Violence Against Women*, *26*(15–16), 1828–1854. https://doi.org/10.1177/1077801219875821

Hertlein, K. M., Eddy, B. P., & Lancaster Strickland, M. (2020). A Framework for Assessing Technology-Mediated IPV. *Journal of Couple and Relationship Therapy*, *19*(4), 296–321. https://doi.org/10.1080/15332691.2020.1838377

Hinduja, S. and Patchin, J. W. (2020) 'Digital Dating Abuse Among a National Sample of U.S. Youth', *Journal of Interpersonal Violence*, pp. 1–21. doi: 10.1177/0886260519897344.

Holt, T. J., & Bossler, A. M. (2020). *The Palgrave Handbook of International Cybercrime and Cyberdeviance*.

Home Office (2021). Domestic Abuse Act: Factsheet https://homeofficemedia.blog.gov.uk/2021/04/29/domesticabuseactfactsheet/

Horvath, M., Alys, L., Massey K., Pina, A., Scally, M. & Adler, J. (2013). "Basically...Porn is everywhere": A Rapid Evidence Assessment on the Effect that Access and Exposure to Pornography has on Children and Young People https://www.childrenscommissioner.gov.uk/report/basically-porn-is-everywhere/

Kaspersky Security Network (2019). *Number of users that encountered "stalkerware" increased by 35% in 2019.* https://www.kaspersky.com/about/press-releases/2019_number-of-users-that-encountered-stalkerware-increased-by-35-percent-to-37000-in-2019

Kaspersky Security Network (2020). *The state of stalkerware in 2020*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2020/03/25175212/EN_The-State-of-Stalkerware-2020.pdf

Kellerman, I., Margolin, G., Borofsky, L. A., Baucom, B. R., & Iturralde, E. (2013). Electronic Aggression Among Emerging Adults: Motivations and Contextual Factors. In *Emerging Adulthood* (Vol. 1, Issue 4, pp. 293–304). SAGE Publications Inc. https://doi.org/10.1177/2167696813490159

Lancaster, M., Seibert, G. S., Cooper, A. N., May, R. W., & Fincham, F. (2020). Relationship Quality in the Context of Cyber Dating Abuse: The Role of Attachment. *Journal of Family Issues*, *41*(6), 739–758. https://doi.org/10.1177/0192513X19881674

Lara, L. (2020) 'Cyber dating abuse: Assessment, prevalence, and relationship with offline violence in young Chileans', *Journal of Social and Personal Relationships*, 37(5), pp. 1681–1699. doi: 10.1177/0265407520907159.

Law Commission (2018.). *Abusive and Offensive Online Communications: A Scoping Report HC 1682 Law Com No 381*.

Laxton, C. (2014). Virtual world, real fear. Women's aid report into online abuse, harassment and stalking. https://www.womensaid.org.uk/virtual-world-real-fear/

Leitão, R. (2019a). Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums. *Human-Computer Interaction*. https://doi.org/10.1080/07370024.2019.1685883

Leitão, R. (2019b). Anticipating smart home security and privacy threats with survivors of intimate partner abuse. *DIS 2019 - Proceedings of the 2019 ACM Designing Interactive Systems Conference*, 527–539. https://doi.org/10.1145/3322276.3322366

Leitão, R. (2018). Digital technologies and their role in intimate partner violence. *Conference on Human Factors in Computing Systems - Proceedings*, *2018-April*. https://doi.org/10.1145/3170427.3180305

Levy, K., & Schneier, B. (2020). Privacy threats in intimate relationships. *Journal of Cybersecurity*, *6*(1), 1–13. https://doi.org/10.1093/CYBSEC/TYAA006

López-Cepero, J., Vallejos-Saldarriaga, J., & Merino-García, M. (2018). Digital Intimate Partner Violence Among Peruvian Youths: Validation of an Instrument and a Theoretical Proposal. *Journal of Interpersonal Violence*. https://doi.org/10.1177/0886260518803610

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G. & Tanczer, L. (2019). 'Internet of Things': How abuse is getting smarter. Safe- The Domestic Abuse Quarterly, (63), 22-26.

Lu, Y., van Ouytsel, J., Walrave, M., Ponnet, K., & Temple, J. R. (2018). Cross-sectional and temporal associations between cyber dating abuse victimization and mental health and substance use outcomes. *Journal of Adolescence*, *65*, 1–5. https://doi.org/10.1016/j.adolescence.2018.02.009

Lyndon, A., Bonds-Raacke, J., & Cratty, A. D. (2011). College students' Facebook stalking of ex-partners. *Cyberpsychology, Behavior, and Social Networking*, *14*(12), 711–716. https://doi.org/10.1089/cyber.2010.0588

Machimbarrena, J. M., Calvete, E., Fernández-González, L., Álvarez-Bardón, A., Álvarez-Fernández, L., & González-Cabrera, J. (2018) 'Internet risks: An overview of victimization in cyberbullying, cyber dating abuse, sexting, online grooming and problematic internet use', *International Journal of Environmental Research and Public Health*, 15(11). doi: 10.3390/ijerph15112471.

Maple, C., Short, E., Brown, A. (2011) *Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey*. https://uobrep.openrepository.com/handle/10547/270578

March, E., Litten, V., Sullivan, D. H., & Ward, L. (2020). Somebody that I (used to) know: Gender and dimensions of dark personality traits as predictors of intimate partner cyberstalking. *Personality and Individual Differences*, *163*. https://doi.org/10.1016/j.paid.2020.110084

Marganski., A. J. & Melander, L. A. (2015). Intimate partner violence victimisation in the cyber and real world: examining the extent of cyber aggression experiences and its association with in-person dating violence. *Journal of Interpersonal Violence, 33*(7). DOI:10.1177/0886260515614283

Melander, L. A. (2010). College students' perceptions of intimate partner cyber harassment. *Cyberpsychology, Behavior, and Social Networking, 13*(3), 263–268. http://dx.doi.org/10.1089/cyber.2009.0221.

Melander, L. and Hughes, V. (2018) 'College partner violence in the digital age: Explaining cyber aggression using routine activities theory', *Partner Abuse*, 9(2), pp. 158–180. doi: 10.1891/1946-6560.9.2.158.

Melander, L. A., & Marganski, A. J. (2020). Cyber and in-person intimate partner violence victimization: Examining maladaptive psychosocial and behavioral correlates. *Cyberpsychology*, *14*(1). https://doi.org/10.5817/CP2020-1-1

Messing, J., Bagwell-Gray, M., Brown, M. L., Kappas, A., & Durfee, A. (2020) 'Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement', *Journal of Family Violence*, 35(7), pp. 693–704. doi: 10.1007/s10896-019-00114-7.

Mishna, F., Lacombe-Duncan, A., Daciuk, J., Fearing, G. & Van Wert, M. (2018) 'Social media, cyber-aggression and student mental health on a university campus', *Journal of Mental Health*, 27(3), pp. 222–229. doi: 10.1080/09638237.2018.1437607.

National Domestic Abuse Helpline (2020). *Covid-19 Special Report.* https://www.thehotline.org/wp-content/uploads/media/2020/09/The-Hotline-COVID-19-60-Day-Report.pdf

NPR (2014). *Smartphones Are Used To Stalk, Control Domestic Abuse Victims*. https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims

Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. *ACM International Conference Proceeding Series*, 1–15. https://doi.org/10.1145/3368860.3368861

Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*. https://citizenlab.ca/docs/stalkerware-holistic.pdf

Perry, J. (2012). *Digital stalking: A guide to technology risks for victims*. Network for Surviving Stalking and Women's Aid Federation joint publication. https://www.womensaid.org.uk/wp-content/uploads/2015/11/Digital_Stalking_Guide_V2_Nov_2012.pdf

Pew Research Centre (2017). *Online Harassment 2017.*

https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

Pineda, D., Galán, M., Martínez-Martínez, A., Campagne, D. M., & Piqueras, J. A. (2021). Same Personality, New Ways to Abuse: How Dark Tetrad Personalities Are Connected With Cyber Intimate Partner Violence. *Journal of Interpersonal Violence*. https://doi.org/10.1177/0886260521991307

Powell, A. and Henry, N. (2018) 'Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives', *Policing and Society*, 28(3), pp. 291–307. doi: 10.1080/10439463.2016.1154964.

Powell, A., & Henry, N. (2019). Technology-Facilitated Sexual Violence Victimization: Results from an online survey of Australian adults. *Journal of Interpersonal Violence, 34*(17) DOI: 10.1177/0886260516672055.

Reed, L. A., McCullough Cosgrove, J., Sharkey, J. D. & Felix, E. (2020) 'Exploring latinx youth experiences of digital dating abuse', *Social Work Research*, 44(3), pp. 157–168. doi: 10.1093/swr/svaa011.

Reed, E., Salazar, M., Behar, A. I., Agah, N., Silverman, J. G., Minnis, A. M., Rusch, M. L. A., & Raj, A. (2019). Cyber Sexual Harassment: Prevalence and association with substance use, poor mental health, and STI history among sexually active adolescent girls. *Journal of Adolescence*, *75*, 53–62. https://doi.org/10.1016/j.adolescence.2019.07.005

Reed, L. A., Tolman, R. M., & Safyer, P. (2015). Too close for comfort: Attachment insecurity and electronic intrusion in college students' dating relationships. *Computers in Human Behavior*, *50*, 431–438. https://doi.org/10.1016/j.chb.2015.03.050

Reed, L. A., Tolman, R. M., & Ward, L. M. (2016). Snooping and Sexting: Digital Media as a Context for Dating Aggression and Abuse Among College Students. *Violence Against Women*, *22*(13), 1556–1576. https://doi.org/10.1177/1077801216630143

Refuge (2020). *70% of refuge service users identify experiencing tech abuse.* https://www.refuge.org.uk/72-of-refuge-service-users-identify-experiencing-tech-abuse/

Ross, J. M., Drouin, M., & Coupe, A. (2019). Sexting Coercion as a Component of Intimate Partner Polyvictimization. *Journal of Interpersonal Violence*, *34*(11), 2269–2291. https://doi.org/10.1177/0886260516660300

Rothman, E. F., Cuevas, C. A., Mumford, E., A., Bahrami, E. & Taylor, B. G. (2021) 'The Psychometric Properties of the Measure of Adolescent Relationship Harassment and Abuse (MARSHA) With a Nationally Representative Sample of U.S. Youth', *Journal of Interpersonal Violence*. doi: 10.1177/0886260520985480.

Roundy, K. A., Mendelberg, P. B., Dell, N., McCoy, D., Nissani, D., Ristenpart, T., & Tamersoy, A. (2020). The many kinds of creepware used for interpersonal attacks. *Proceedings - IEEE Symposium on Security and Privacy*, *2020-May*, 626–643. https://doi.org/10.1109/SP40000.2020.00069

Sánchez, V., Muñoz-Fernández, N., & Ortega-Ruíz, R. (2015). "Cyber dating Q_A": An instrument to assess the quality of adolescent dating relationships in social networks. *Computers in Human Behavior, 48*, 78–86.https://doi.org/10.1016/j.chb.2015.01.006.

Schnurr, M. P., Mahatmya, D., & Basche, R. A. (2013). The role of dominance, cyber aggression perpetration, and gender on emerging adults' perpetration of intimate partner violence. *Psychology of Violence*, *3*(1), 70–83. https://doi.org/10.1037/a0030601

Smoker, M., & March, E. (2017). Predicting perpetration of intimate partner cyberstalking: Gender and the Dark Tetrad. *Computers in Human Behavior*, *72*, 390–396. https://doi.org/10.1016/j.chb.2017.03.012

Statista (2021a). *Global Digital Population as of January 2021* https://www.statista.com/statistics/617136/digital-population-worldwide/

Statista (2021b) *Mobile social media worldwide- statistics and facts*. https://www.statista.com/topics/2478/mobile-social-networks/

Stonard, K. E., Bowen, E., Walker, K., & Price S. A. (2017). "They'll Always Find a Way to Get to You": Technology Use in Adolescent Romantic Relationships and Its Role in Dating Violence and Abuse, *Journal of Interpersonal Violence, 32*(14). doi: 10.1177/0886260515590787.

Strickland, P., & Dent, J. (2017). *Online harassment and cyber bullying*. www.parliament.uk/commons-library|intranet.parliament.uk/commons-library|papers@parliament.uk|@commonslibrary

Tanczer, L., Lopez-Neira, I., Parkin, S., Patel, T., & Danezis, G. (2018). Gender and IoT Research Report: Internet of Things and implications for technology facilitated abuse. https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf

Taylor, S., & Xia, Y. (2018). Cyber Partner Abuse: A Systematic Review. *Violence and Victims*, *33*(6), 983–1011. https://doi.org/10.1891/0886-6708.33.6.983

Tolan, C. (2020) *Some cities see jumps in domestic violence during the pandemic. CNN* https://edition.cnn.com/2020/04/04/us/domestic-violence-coronavirus-calls-cases-increase-invs/index.html

Trujillo, O., Cantu, J. I., & Charak, R. (2020). Unique and Cumulative Effects of Intimate Partner Cybervictimization Types on Alcohol Use in Lesbian, Gay, and Bisexual Emerging Adults. *Cyberpsychology, Behavior, and Social Networking*, *23*(11), 743–751. https://doi.org/10.1089/cyber.2019.0773

Tseng, E., Freed, D., Engel, K., Ristenpart, T. & Dell , N. (2021). *A digital security dilemma: Analysis of computer-mediated computer security interventions for intimate partner violence during COVID-19.* In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 17 pages. https: //doi.org/10.1145/3411764.3445589

van Gelder, N., Potts, A., O'Donnell, M., Thompson, K., Shah, N., Oertelt-Prigione, S. (2020). COVID-19: Reducing risk of infection might increase the risk of intimate partner violence. EClinical Medicine (21) https://doi.org/10.1016/j.eclinm.2020.100348

van Ouytsel, J., Ponnet, K., Walrave, M., & Temple, J. R. (2016). Adolescent cyber dating abuse victimization and its associations with substance use, and sexual behaviors. *Public Health*, *135*, 147–151. https://doi.org/10.1016/j.puhe.2016.02.011

Villora, B., Yubero, S., & Navarro, R. (2019). Associations between feminine gender norms and cyber dating abuse in female adults. *Behavioral Sciences*, *9*(4). https://doi.org/10.3390/bs9040035

Vitis, L. (2020) 'Private, Hidden and Obscured: Image-Based Sexual Abuse in Singapore', *Asian Journal of Criminology*, 15(1), pp. 25–43. doi: 10.1007/s11417-019-09293-0.

Watkins, L. E., Benedicto, R. C., Brockdorf, A., & DiLillo, D. (2020). Physical and Sexual Intimate Partner Aggression Among College Students: Examining the Roles of Cyber Intimate Partner Aggression and Alcohol Use. *Journal of Interpersonal Violence*. https://doi.org/10.1177/0886260520912593

Watkins, L. E., Maldonado, R. C., & DiLillo, D. (2018). The Cyber Aggression in Relationships Scale: A New Multidimensional Measure of Technology-Based Intimate Partner Aggression. *Assessment*, *25*(5), 608–626. https://doi.org/10.1177/1073191116665696

Weathers, M. R., Canzona, M. R., & Fisher, C. L. (2019). Digital Media as a Context for Dating Abuse: Connecting Adaptive and Maladaptive Coping Strategies to Young Adult Women's Well-Being. *Affilia - Journal of Women and Social Work*, *34*(3), 325–345. https://doi.org/10.1177/0886109919832005

Weathers, M. R., & Hopson, M. C. (2015). "I Define What Hurts Me": A Co-Cultural Theoretical Analysis of Communication Factors Related to Digital Dating Abuse. *Howard Journal of Communications*, *26*(1), 95–113. https://doi.org/10.1080/10646175.2015.988475

Whitton, S. W., Dyar, C., Mustanski, B. & Newcomb, M. E. (2019). 'Intimate Partner Violence Experiences of Sexual and Gender Minority Adolescents and Young Adults Assigned Female at Birth', *Psychology of Women Quarterly*, 43(2), pp. 232–249. doi: 10.1177/0361684319838972.

Witwer, A. R., Langton, L., Vermeer, M. J. D., Banks, D., Woods, D., & Jackson, B. A. (2020). *Countering Technology-Facilitated Abuse: Criminal Justice Strategies for Combating Nonconsensual Pornography, Sextortion, Doxing, and Swatting*. Rand Corporation https://www.rand.org/pubs/research_reports/RRA108-3.html

Wolford-Clevenger, C. , Zapor, H., Brasfield, H., Febres, J., Elmquist, J., Shorey, R. & Stuart, G. L. (2016). An examination of the partner cyber abuse questionnaire in a college student sample. *Psychology of Violence*, 6(1), pp. 156–162. doi: 10.1037/a0039442.

Women's Aid (2020). Women's Aid and Privacy International launch digital information cards to help women stay safe. https://www.womensaid.org.uk/womens-aid-and-privacy-international-launch-digital-information-cards-to-help-women-stay-safe-on-valentines-day/

Women's Safety New South Wales (2020). *Impact of COVID-19 on migrant and refugee women and chidlren experiencing DFV.* https://www.womenssafetynsw.org.au/impact/publication/impact-of-covid-19-on-migrant-and-refugee-women-and-children-experiencing-dfv/

Wood, L., Voth Schrag, R. & Busch- Armendariz, N. (2020). Mental health and academic impacts of intimate partner violence among IHE-attending women, J*ournal ofAmerican College Health, 68(*3), 286-293, DOI: 10.1080/07448481.2018.1546710

Woodlock, D. (2017). The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women*, *23*(5), 584–602. https://doi.org/10.1177/1077801216646277

Woodlock, D., McKenzie, M., Western, D., & Harris, B. (2020). Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control. *Australian Social Work*, *73*(3), 368–380. https://doi.org/10.1080/0312407X.2019.1607510

World Health Organisation (WHO; 2021) *Violence Against Women.* https://www.who.int/news-room/fact-sheets/detail/violence-against-women

Worsley, J. D., Wheatcroft, J., Short, E. & Corcoran, R. (2017). Victims voices: Understanding the emotional impact of cyberstalking and individuals' coping responses. SAGE Open, 7 (2)DOI. 10.1177/2158244017710292

Yahner, J., Dank, M., Zweig, J., & Lachman, P. (2015). The co-occurrence of physical andcyber dating violence and bullying among teens. *Journal of Interpersonal Violence,30*(7), 1079–1089. https://doi.org/10.1177/0886260514540324.

Yardley, E. (2020). Technology-Facilitated Domestic Abuse in Political Economy: A New Theoretical Framework. *Violence Against Women*. https://doi.org/10.1177/1077801220947172

Zattoni, F., Gül, M., Soligo, M., Morlacco, A., Motterle, G., Collavino, J., Barneschi, A. C., Moschini, M., & Moro, F. D. (2020). The impact of COVID-19 pandemic on pornography habits: a global analysis of Google Trends. International Journal of Impotence Research. https://doi.org/10.1038/s41443-020-00380-w

Zhong, L. R., Kebbell, M. R., & Webster, J. L. (2020). An exploratory study of technology-facilitated Sexual Violence in online romantic interactions: Can the Internet's toxic disinhibition exacerbate sexual aggression? *Computers in Human Behavior*, *108*. https://doi.org/10.1016/j.chb.2020.106314